



BreezeMAX Wi² and BreezeACCESS Wi²

System Manual

SW Version 5.2
August 2008
P/N 215081

Document History

Topic	Description	Date Issued
This is the document's first Release		Version 5.2, June 2007
Wi ² Extender	New hardware	Version 5.2, August 2008
Chapter 3		

Legal Rights

© Copyright 2008 Alvarion Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMANAGE™, BreezeLINK®, BreezeConfig™, BreezeMAX™, AlvariSTAR™, BreezeLITE™, AlvariCRAFT™, MGW™, eMGW™ and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

- (a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.
- (b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from

invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

- (a) THE SUPPLIED UNITS SUPPORT 802.11 b/g ONLY.
- (b) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.
- (c) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE

FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

- (a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- (b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Outdoor Unit and Antenna Installation and Grounding

Ensure that outdoor units, antennas and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast (when using external antenna) are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Disposal of Electronic and Electrical Waste



Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice.
- Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

Some of the equipment provided by Alvarion and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by Alvarion or

the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user's authority to operate the equipment and/or revoke the warranty provided by such manufacturer.



Compliances

NOTE



This section provides regulatory compliance details for the Access Point unit of the system. Refer to the relevant manual for compliance details of the SU-ODU unit.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EC Conformance Declaration

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950 (IEC 60950) - Product Safety
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

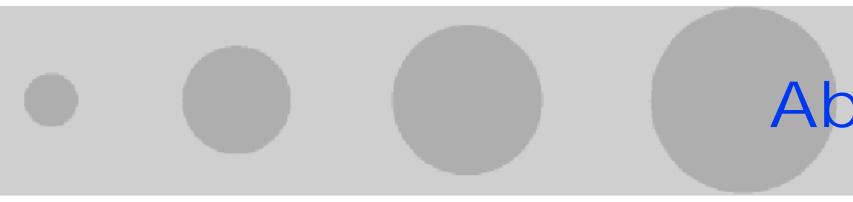
NOTE



The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, outdoor restrictions and license requirements for each European Community country as described in this document.
- This device may be operated in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below.

- » In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- » In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- » In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.



About This Manual

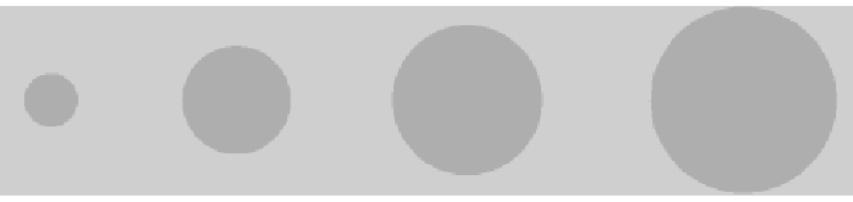
This manual describes the BreezeMAX Wi² and BreezeACCESS Wi² AP and details how to install, operate and manage the access point.

This manual is intended for technicians responsible for installing, setting and operating the BreezeMAX Wi² and BreezeACCESS Wi², and for system administrators responsible for managing the system.

This manual contains the following chapters and appendices:

- **Chapter 1 - Product Description** - Describes the Wi² unit and its functionality.
- **Chapter 2 - Installation** - Describes how to install the Wi² and how to connect to subscriber's equipment.
- **Chapter 3 - Hardware Installation Wi² Extender** - Describes how to install the Wi² Extender.
- **Chapter 4 - Getting Started** - Describes how to initially configure the APs in autonomous mode and establish a connection through the AP to the Internet.
- **Chapter 5 - Working with virtual networks** - Describes how to work with virtual networks.
- **Chapter 6 - Wireless Configuration** - Describes how to work with and configure wireless coverage.
- **Chapter 7 - Network Configuration** - Describes how to configure the network.
- **Chapter 8 - Management** - Describes the management tool that provides easy access to all configuration and monitoring functions.
- **Chapter 9 - Security** - Describes how to use RADIUS servers and manage certificates.
- **Chapter 10 - Local Mesh** - Describes the local mesh feature.

- **Chapter 11 - Maintenance** - Describes the maintenance features available.
- **Appendix A - Troubleshooting** - Provides a list of tasks to perform in case of problems before contacting local Technical Support.
- **Appendix B - Resetting to Factory Defaults** - Describes how to force an AP into its default factory state.



Contents

Chapter 1 - Product Description

1.1	Introduction	2
1.2	Specifications.....	4
1.2.1	Radio	4
1.2.2	Sensitivity	5
1.2.3	8 dBi Omni Antenna	5
1.2.4	Wi ² Solution System SW Features	6
1.2.5	Mechanical	7
1.2.6	Electrical.....	7
1.2.7	Connectors and LEDs	8
1.2.8	Environmental	8
1.2.9	Standards Compliance	9

Chapter 2 - Hardware Installation

2.1	Hardware Description	12
2.1.1	Bottom Panel.....	13
2.1.2	Top Panel	14
2.1.3	LED Indicators.....	14
2.2	Installation Requirements	16
2.2.1	Packing List	16
2.2.2	Additional/Optional Installation Requirements.....	16
2.2.3	Guidelines for Positioning Wi ²	18
2.3	Installation	19
2.3.1	Attaching the SU-ODU to the Mounting Plate	19

2.3.2	Attaching the Mounting Plate to the Wi ² Unit.....	21
2.3.3	Connecting the Wi ² Unit to the SU-ODU	22
2.3.4	Preparing the Power Cable	26
2.3.5	Mounting the Wi ² Unit.....	28
2.3.6	Connecting the Antenna(s).....	31
2.3.7	Connecting the Grounding Cables	31
2.3.8	Connecting to Power Source.....	31
2.3.9	Configuration and Testing	32

[Chapter 3 - Hardware Installation Wi² Extender](#)

3.1	Wi² Extender ODU Hardware Description	36
3.1.1	Ethernet Port	36
3.1.2	Console Port.....	36
3.1.3	Grounding Point	36
3.1.4	Water Tight Test Point.....	36
3.1.5	Pole-Mounting Bracket Attachment Points.....	36
3.1.6	LED Indicators.....	37
3.2	Installation Requirements	38
3.2.1	Packing List	38
3.2.2	Additional/Optional Installation Requirements.....	39
3.2.3	Guidelines for Positioning Wi ² Extender.....	39
3.3	Mounting the Wi² Extender ODU.....	40
3.4	Connecting Cables to the Outdoor Unit.....	45
3.4.1	Grounding Wire	45
3.5	The Power Injector IDU	46
3.6	Connecting the Power Injector IDU Cables	47
3.6.1	Connecting the Antenna(s).....	48

3.6.2	Connecting the Grounding Cables	49
3.6.3	Connecting to Power Source.....	49
3.6.4	Configuration and Testing	49

Chapter 4 - Getting Started

4.1	Introduction	52
4.2	Configuration Procedure.....	53

Chapter 5 - Working with Virtual Networks

5.1	Key Concepts	62
5.1.1	Stand-alone Deployment.....	62
5.1.2	Deployment in Conjunction with an Alvarion Service Controller	66
5.1.3	Management with VLANs.....	67
5.2	Virtual Network Configuration Overview	69
5.2.1	About the 'Use Alvarion Access Controller' Option	70
5.3	Virtual Network Configuration Options.....	72
5.3.1	Virtual AP	72
5.3.2	Egress VLAN.....	73
5.3.3	Wireless Security Filters	74
5.3.4	Wireless Protection	75
5.3.5	MAC-based Authentication.....	78
5.3.6	Location-aware.....	78
5.3.7	Wireless MAC Filter.....	78
5.3.8	Wireless IP Filter	79
5.4	Virtual Network Data Flow.....	80
5.4.1	Stand-alone Deployment.....	81
5.4.2	AP deployed with an Alvarion Service Controller	81

5.4.3	Virtual Network on Service Controller	82
5.5	Quality of Service (QoS)	84
5.5.1	QoS Priority Mechanism.....	84

[Chapter 6 - Wireless Configuration](#)

6.1	Wireless Coverage.....	90
6.1.1	Wireless Mode.....	90
6.1.2	Factors Limiting Wireless Coverage.....	90
6.1.3	Configuring Overlapping Wireless Cells.....	92
6.2	Conducting a Site Survey.....	97
6.2.1	Scanning Frequency	97
6.2.2	Identifying Unauthorized APs	98
6.3	Radio Configuration.....	100
6.3.1	Configuration Parameters	101

[Chapter 7 - Network Configuration](#)

7.1	Port Configuration	108
7.1.1	Port Configuration Information	108
7.1.2	Bridge Port Configuration	109
7.1.3	Port Configuration	110
7.1.4	Wireless Port Configuration.....	111
7.2	VLAN Support.....	112
7.2.1	Using a Default VLAN	112
7.2.2	Assigning Traffic to a VLAN	113
7.2.3	VLAN Bridging.....	113

7.2.4	VLAN Configuration.....	114
7.3	Bandwidth Control	116
7.4	CDP.....	117
7.5	DNS.....	118
7.5.1	DNS Servers	118
7.5.2	DNS Advanced Settings.....	118
7.6	IP Routes.....	120
7.6.1	Configuration	120
7.7	IP QoS	122
7.7.1	Configuration	122
7.7.2	Example	124

[Chapter 8 - Management](#)

8.1	Management Tool.....	128
8.1.1	Management Station	128
8.1.2	Starting the Management Tool.....	128
8.1.3	Customizing Management Tool Settings.....	128
8.2	SNMP	133
8.2.1	Configuring SNMP Settings.....	133
8.3	SOAP	136
8.3.1	Configuring the SOAP Server	136
8.4	CLI	138
8.4.1	Configuring CLI Support.....	138
8.5	System Time	140
8.6	Country	141

[Chapter 9 - Security](#)

9.1	Using a RADIUS Server	144
------------	------------------------------------	------------

9.1.1	Configuring a RADIUS Client Profile on the AP	144
9.1.2	Configuring User Profiles on a RADIUS Server	147
9.1.3	Configuring Administrator Profiles on the RADIUS Server.....	153
9.2	Managing Certificates.....	155
9.2.1	Trusted CA Certificate Store	155
9.2.2	Installing a New CA Certificate.....	156
9.2.3	CA certificate Import Formats.....	156
9.2.4	Default CA Certificates	157
9.2.5	Certificate Usage.....	159
9.2.6	About Certificate Warnings.....	160

[Chapter 10 - Local Mesh](#)

10.1	Key Concepts	164
10.1.1	New in this Release.....	164
10.1.2	Benefits	164
10.2	Local Mesh Terminology	165
10.2.1	Static Local Mesh Links.....	165
10.2.2	Dynamic Local Mesh Links.....	165
10.3	Local Mesh Profiles	169
10.3.1	Configuring a Local Mesh Profile	170
10.4	Configuration Considerations	178
10.4.1	Simultaneous AP and Local Mesh	178
10.4.2	Maximum Range	178
10.5	Quality of Service.....	179
10.6	Configuration Summary	180
10.7	How to Configure Local Mesh in Controlled Mode	181
10.7.1	Setting a Master Profile	181

10.7.2	Setting the Master AP	186
10.7.3	Setting the SLAVE AP.....	187
10.7.4	Adding the Slave AP in a Group on the Controller	190
10.7.5	Operation Verification.....	193
10.8	Sample Local Mesh Deployments	195
10.8.1	Dynamic Networks	195
Chapter 11 - Maintenance		
11.1	Config File Management.....	198
11.1.1	Manual Configuration File Management	198
11.1.2	Scheduled Operations.....	200
11.1.3	Managing the Configuration File with cURL.....	201
11.2	Firmware Updates	204
11.2.1	Immediate Update	205
11.2.2	Scheduled Update.....	205
11.2.3	Updating Firmware with cURL.....	206
11.3	Licenses.....	207
11.3.1	Factory Reset Considerations	208
Appendix A - Troubleshooting		
Appendix B - Resetting to Factory Defaults		
B.1	Introduction	216
B.1.1	Using the Reset Switch	216
B.1.2	Using the Management Tool	216
B.1.3	Using Special Commands	218

Chapter 1 - Product Description

In This Chapter:

- “Introduction” on page 2
- “Specifications” on page 4

1.1 Introduction

Alvarion's Wi² suite of converged solutions, including BreezeMAX Wi² and BreezeACCESS Wi²("Wi²"), unites the advantages of the popular WiFi access with the powerful capabilities of BreezeMAX or BreezeACCESS VL/4900 ("BreezeACCESS") systems to provide cost-effective solutions for personal broadband services.

The Wi² system comprises a self-contained combination of an advanced WiFi access point and a BreezeMAX or BreezeACCESS SU-ODU that provides backhaul connectivity. With its advanced roaming software, the Wi² can be deployed almost anywhere to provide broadband mobility to standard WiFi (IEEE 802.11 b/g) end user devices. Used in conjunction with Alvarion's market-leading BreezeMAX or BreezeACCESS base stations, the Wi² can be used to expand the existing capabilities of Alvarion's WiMAX and pre-WiMAX networks. Using the Wi², a BreezeMAX or BreezeACCESS network can be used to provide personal broadband services to high-end business as well as residential users equipped with WiFi enabled devices such as laptops, PDAs, smart-phones, and portable gaming devices. As a converged system, the Wi² also gives operators the ability to seamlessly transition to a fully mobile WiMAX network with managed services for personal broadband users.

Operating in both licensed and licensed-exempt frequencies, the Wi² system leverages the easy availability of WiFi technology - along with the power and robustness of BreezeMAX or BreezeACCESS broadband wireless access system - to answer critical public and private sector needs such as traffic management, video surveillance, public Internet access, homeland security, and various nomadic applications.

The Wi² is a self-contained, robust all-outdoor system that comprises three elements:

- A feature-rich WiFi (IEEE 802.11 b/g) Access Point (AP)
- A BreezeMAX/BreezeACCESS VL/BreezeACCESS 4900 SU-ODU (supplied separately).

NOTE



In a BreezeACCESS VL/4900 backhauling link, an SU-54-BD model should be used.

- A power supply module that provides power to both the WiFi AP and the SU-ODU.

The Wi² system requires only a single connection to either AC or DC power. With its easy installation and operation, high performance, and rich security and QoS feature sets, the Wi² is an ideal solution for operators, municipalities and communities looking to build metropolitan broadband networks or to integrate WiFi hot zone capabilities into their existing broadband wireless access networks. The result is personal broadband services ranging from public Internet access to public safety and Intranet applications.

NOTE



This document describes how to install and manage the Wi² system, including the installation and connections of a BreezeMAX or BreezeACCESS SU-ODU when installed on the mounting plate of the Wi² system. For details on other installation options for the SU-ODU and how to manage it, refer to the relevant *BreezeMAX* or *BreezeACCESS VL/4900* documents.

1.2 Specifications

1.2.1 Radio

Item	Description
Radio Type	IEEE 802.11b/g
Radio Mode	802.11b+g, 802.11b only, 802.11g only
Frequency Band	2400-2497 MHz
Operating Channels	ETSI (EUR): 2412 ~ 2472 MHz(CH1-CH13) MKK (Japan) 11b: 2412 ~ 2484 MHz (CH1-CH14) MKK (Japan) 11g: 2412 ~ 2472 MHz(CH1-CH13) France: (CH1-CH13)
Channel Bandwidth	20 MHz
Data Rates	802.11b: 1, 2, 5.5, 11 Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b Radio Technology	Direct Sequence-Spread Spectrum (DSSS)
802.11b Modulation Technique	Differential Binary Phase Shift Keying (DBPSK) @ 1 Mbps Differential Quadrature Phase Shift Keying (DQPSK) @ 2 Mbps Complementary Code Keying (CCK) @ 5.5 and 11 Mbps
802.11g Radio Technology	Orthogonal Frequency Divisional Multiplexing (OFDM)
802.11g Modulation Technique	Binary Phase Shift Keying (BPSK) @ 6 and 9 Mbps Quadrature Phase Shift Keying (QPSK) @ 12 and 18 Mbps 16-Quadrature Amplitude Modulation (QAM) @ 24 & 36 Mbps 64-QAM @ 48 & 54 Mbps
FEC Coding Rates	1/2 2/3, 3/4
Max Tx Power	6 to 24 Mbps: 20dBm. 36 and 48 Mbps: 19dBm. 54 Mbps: 18dBm 802.11b for all frequencies and all rates: 20dBm.
TPC (Transmit Power Control)	0% - 100%
Antenna Ports	2 x N-Type, 50 ohm
Antenna Diversity	Rx antenna switching by energy sensing

1.2.2 Sensitivity

Data Rate	Sensitivity (dBm)
802.11b, 1 Mbps	-96
802.11b, 2 Mbps	-93
802.11b, 5.5 Mbps	-93
802.11b, 11 Mbps	-90
802.11g, 6 Mbps	-91
802.11g, 9 Mbps	-90
802.11g, 12 Mbps	-89
802.11g, 18 Mbps	-88
802.11g, 24 Mbps	-84
802.11g, 36 Mbps	-80
802.11g, 48 Mbps	-75
802.11g, 54 Mbps	-73

1.2.3 8 dBi Omni Antenna

Item	Description
Antenna gain	8 dBi
VSWR	2:1 max
Antenna Polarization	Linear Vertical
Horizontal Plane	360°
Vertical Plane	15°
Dimensions	52 cm x 1.9 cm diameter
Weight	340 g

1.2.4 Wi² Solution System SW Features

Item	Description
Access Control	<ul style="list-style-type: none"> ■ Integrated HTML login/captive portal ■ Integrated RADIUS authentication ■ Configurable min./max. connect speed ■ Scalable to thousands of users
Centralized Management	<ul style="list-style-type: none"> ■ Full plug and play AP configuration, upgrade and control ■ Centralized system monitor for thousands of APs ■ Full, secure GUI configuration and monitoring
Management	<ul style="list-style-type: none"> ■ SNMP, CLI, web-based ■ Selectable RF channel and transmit power ■ Packet capture on WLAN or LAN ■ interface (diagnostics)
Multiservice	<ul style="list-style-type: none"> ■ Support for 16 virtual networks, hidden and broadcast SSIDs ■ Unique SSID, Mac address, authentication, encryption, VLANs and QoS ■ Per-user bandwidth management ■ User account profiles using embedded/external AAA ■ Full virtual AP configuration, including authentication, DTIM, QoS
Mobility	<ul style="list-style-type: none"> ■ Full voice quality L2 and L3 mobility for clients roaming between APs ■ Service transparency through fast roaming and handovers
QoS and Other	<ul style="list-style-type: none"> ■ Support for 802.11i, WMM, RADIUS, 802.1q, 802.1p, IP TOS/DSCP ■ Mesh (DWDS), self-healing, selfoptimizing

Item	Description
Security	<ul style="list-style-type: none"> ■ 802.1x, AES, WPA2, Radius, WEP, Firewall ■ SSH/SSL, IPSec encapsulated ■ SNMP, XML ■ Wireless MAC/IP filter, NAT, CIDR ■ Layer-2 wireless client isolation ■ DHCP: Server; Client; Relay, Option 82, Rogue AP detection and prevention

1.2.5 Mechanical

Item	Description
Dimensions (excluding mounting plate and connectors)	240mm (W) X 261mm (H) X 171mm (D)
Weight (excluding antennas, backhauling CPE and mounting plate)	4.85 Kg
Weight of Mounting Plate	0.7 Kg
AC Power Supply	85-260VAC, 47-63Hz, maximum power consumption 2.5A
Mounting Plate Tilt	+/- 15°
Mounting Plate Rotation	+/- 45°

1.2.6 Electrical

Type	Details
AC Power Supply	85-260VAC, 47-63Hz, maximum power consumption 2.5A
DC Power supply	42 VDC to 60 VDC, maximum power consumption 3.5A
AC/DC Power Switching	When both AC and DC power sources are connected, AC power input will be used as long as internal power supplies are working properly. The unit will switch to DC power source if AC power input fails, or the internal power supplies fail, and the DC power input is in the proper range.

1.2.7 Connectors and LEDs

Type	Description
AC IN	Connection to AC mains. 3-pin power plug, Bulgin PX0732/S/07
SU	Ethernet and power connection to backhauling CPE. RJ-45, in a weather protected service box
AP	Ethernet and power connection to AP (PoE). RJ-45, in a weather protected service box
DC IN	Connection to DC power source. 2-pin power plug, Bulgin PX0736/S/07
PoE	Ethernet and power connection, 8-pins DIN jack 10/100Base-T, half/full duplex with auto-negotiation
Console	RS232 DTE, 8-pins DIN jack
LEDs	<ul style="list-style-type: none"> ■ Power ■ Link (Ethernet link integrity/activity) ■ 11b/g: 3 LEDs indicating wireless link activity

1.2.8 Environmental

Item	Details
Operating Temperature	-40 ⁰ C to 55 ⁰ C
Storage Temperature	-40 ⁰ C to 70 ⁰ C
Humidity	Maximum 95%.
Water Proof	IP-67
Solar Radiation protection	IEC 60068-2-5
Salt	IEC 60068 part 2-52
Transportation	ETS 300 019-2-2 Class 2.3 Public Transportation
Storage shock	IEC 68-2-29
Storage drop	IEC 68-2-32
Wind operation	160 Km/hour
Wind survival	220 Km/hour

1.2.9 Standards Compliance

Type	Standard
EMC	<ul style="list-style-type: none">■ EN55022 CE Class B■ FCC Class B Part 15
Safety	<ul style="list-style-type: none">■ UL / CUL (CSA60950-1, UL60950-1)■ CE / CB (EN60950/IEC 60950-1)
Lightning	The unit withstand at +4KV of Input surge, 1.2usec rise/fall time, 50μsec duration, every 10 seconds, for all interfaces.
Radio	<ul style="list-style-type: none">■ ETSI 300 328 (11b/g)■ ETSI 301 489 (DC power)■ FCC Part 15C 15.247/15.207 (11b/g)■ RS210 (Canada)■ TELEC



2

Chapter 2 - Hardware Installation

In This Chapter:

- “Hardware Description” on page 12
- “Installation Requirements” on page 16
- “Installation” on page 19
 - » “Attaching the SU-ODU to the Mounting Plate” on page 19
 - » “Attaching the Mounting Plate to the Wi² Unit” on page 21
 - » “Connecting the Wi² Unit to the SU-ODU” on page 22
 - » “Preparing the Power Cable” on page 26
 - » “Mounting the Wi² Unit” on page 28
 - » “Connecting the Antenna(s)” on page 31
 - » “Connecting the Grounding Cables” on page 31
 - » “Connecting to Power Source” on page 31
 - » “Configuration and Testing” on page 32

2.1 Hardware Description

The Wi² consists of a WiFi access point with an integrated power supply and interface module that connects to either a BreezeMAX or BreezeACCESS outdoor unit (SU-ODU) for backhaul and network management software. Each unit is housed in a weatherproof enclosure for mounting outdoors.

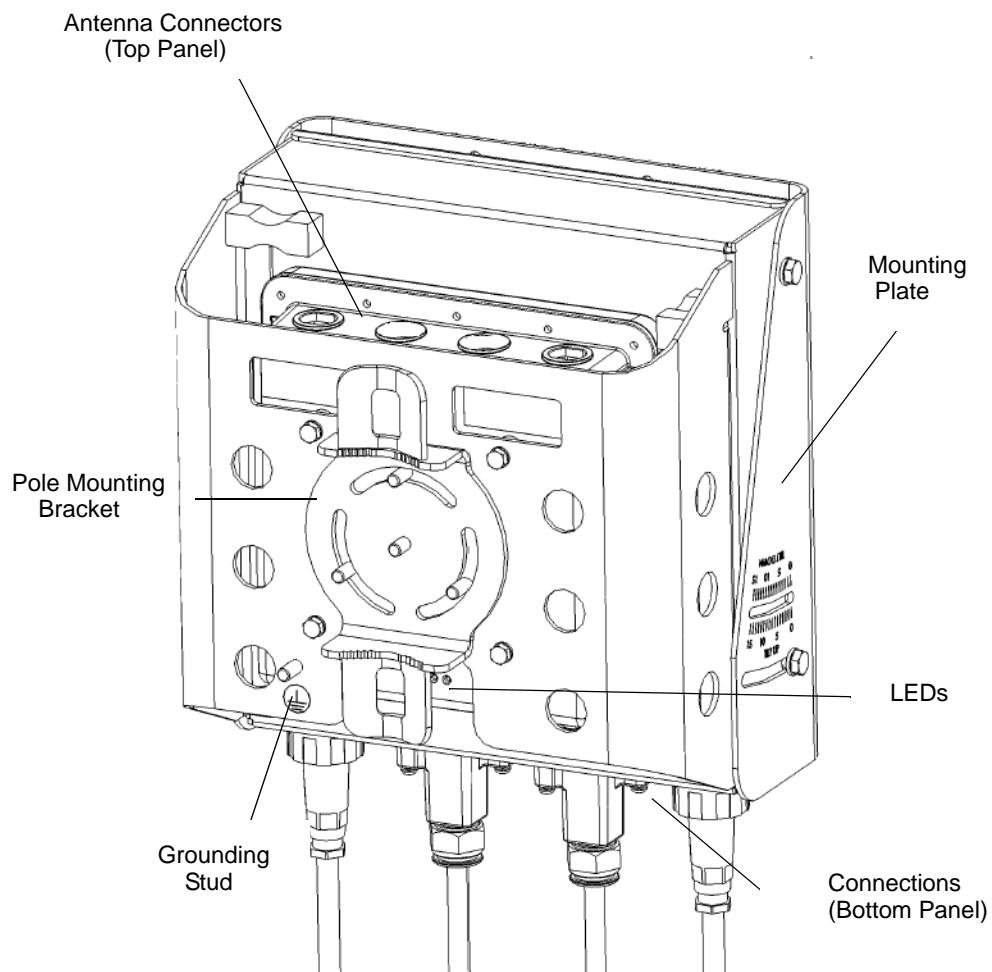


Figure 2-1: Wi² Unit (without SU-ODU)

NOTE



The diagram in [Figure 2-1](#) includes a mounting plate for an SU-ODU. (It does not show the actual SU-ODU). The SU-ODU can also be installed separately, in which case there is no need to attach the mounting plate to the Wi² unit.

2.1.1 Bottom Panel

[Figure 2-2](#) shows the bottom panel of the Wi² unit and the table below lists the components.

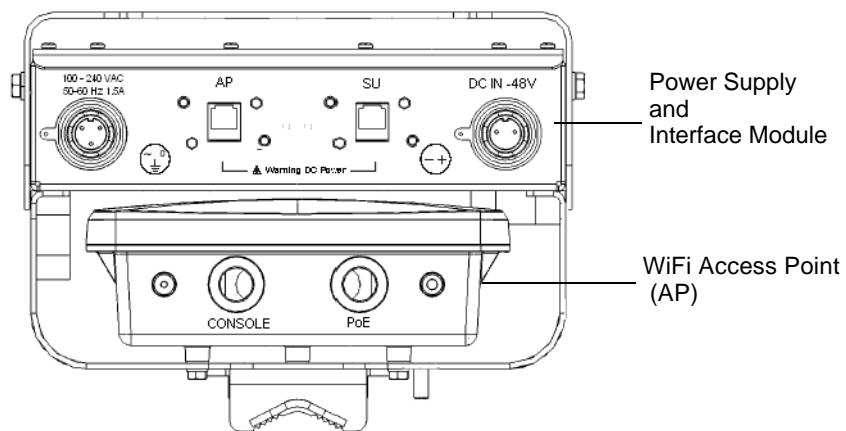


Figure 2-2: Bottom Panel (without the SU-ODU)

Element	Item	Description
WiFi Access Point (AP)	Console Port Cover Holder	Holder for waterproof protection cover for console port when port is not in use.
	Console Port	Connection to console port for system management.
	PoE Port	An Ethernet cable connects the PoE port to the AP port in the Power Supply and Interface Module.
	Impermeability Test Screw	Do not remove or loosen this screw. Doing so may impair the sealing of the unit against moisture and humidity.
Power Supply and Interface Module	AC Power Plug	3-pin power plug for connection to AC power source.
	AP Port	An Ethernet cable connects the AP port to the PoE port in the AP.
	SU Port	Connection to BreezeMAX or BreezeACCESS outdoor unit
	DC Power Plug	2-pin power plug for connection to DC power source.

2.1.2 Top Panel

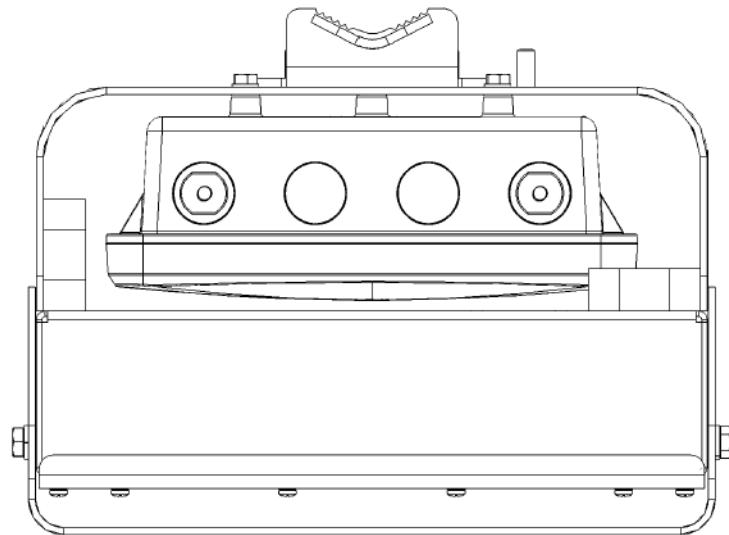


Figure 2-3: Top Panel (without the SU-ODU)

Figure 2-3 shows the top panel of the Wi² unit with two N-type RF connectors for external antennas.

2.1.3 LED Indicators

The Wi² includes eight status LED indicators. Figure 2-4 shows the LEDs and the table below describes the system status.

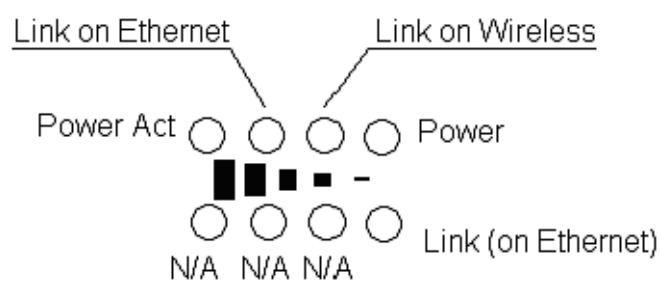


Figure 2-4: LED Indicators

2.1.3.1 Autonomous Mode

The status lights provide the following information when a AP is operating in autonomous mode:

Status Light	State	Description
Power Act	Off	There is no power to the WI2SR-1.
	Flashing	The WI2-SR-1 is starting up.
	Solid	The WI2-SR-1 is fully operational.
Link on Ethernet	Off	Port is not connected or there is no activity.
	Flashing	Ethernet port is transmitting or receiving.
	Solid	The light comes on for a short period when the link is established.
Link on Wireless	Flashing	Wireless port is receiving data.
Power	Solid	When the WI2-SR-1 is plugged in.

2.1.3.2 Controlled Mode

The status lights provide the following information when an AP is operating in controlled mode:

Status Light Behavior	Description
Power Act blinks slowly.	WI2-SR-1 is looking for an IP address
Power Act, Link on Ethernet, and Link on Wireless light each turn ON and OFF one after the other, giving the impression of movement from left to right	WI2-SR-1 has obtained an IP address and is attempting to discover a WI2-SR-CTRL.
Power Act light is solid. Link on Ethernet blinks until the tunnel is established.	WI2-SR-1 has found a WI2-SR-CTRL and is attempting to establish a secure tunnel with it.
Power Act light and Link on Ethernet light blink alternatively and quickly. Wireless light is off.	WI2-SR-1 has received a discovery reply from two or more WI2-SR-CTRLs with the same priority setting. The WI2-SR-1 is unable to connect with either until the priority conflict is resolved.

Once the AP has established a secure tunnel with a CTRL, the status lights revert to their normal operation:

- Power light is solid to indicate that the AP is fully operational
- Ethernet light blinks to indicate the presence of traffic on the Ethernet port
- Wireless light blinks to indicate the presence of traffic on the wireless port

2.2 Installation Requirements

This section describes all the supplies required to install the Wi² and the items included in each installation package.

2.2.1 Packing List

The BreezeMAX Wi² and BreezeACCESS Wi² installation kit includes the following components:

- Wi² unit
- SU-ODU mounting plate
- 4 sets of M8 x 16 hex head screws + flat washers + spring washers
- 4 sets of 1/4" x 1/2" hex head screws + flat washers + spring washers
- 4 sets of M6 x 12 hex head screws + flat washers + spring washers
- Cable kit including a 55 cm category 5E Ethernet cable with two shielded RJ-45 connectors, one with a metal service box, and a spare shielded RJ-45 connector.
- AC power connector
- 2 x 9/16" (530 mm) metal bands
- 3m Ethernet configuration cable (2 pairs, straight)

2.2.2 Additional/Optional Installation Requirements

- Category 5E cable* for connecting to an SU-ODU if installed separately (maximum length 100m.)
- Rubber sealing cap for BreezeMAX or BreezeACCESS HW Revision E ODU (supplied with SU-ODU)
- Service Box for BreezeACCESS HW Revision D or lower ODU (supplied with SU-ODU).

- Crimping tool for RJ-45 connectors (if connecting to a BreezeACCESS ODU)
- RS232 console cable*
- 8 dBi Omnidirectional antenna(s)*
- Sectoral antenna(s), including RF cable with N-Type connector*
- UL/CSA listed smooth circular power cable, 1.5mm to 2.5mm each. Outer diameter 7mm to 9mm, UV resistant, temperatures range -40⁰C to +65⁰C min. Other specifications (such as oil resistance, no of wires) according to specific installation requirements.
- A mains plug for connecting to AC mains
- Two terminal rings if connecting to a DC source
- Grounding cable with an appropriate termination.
- Installation tools and materials, including appropriate means for installing the Wi² and antenna(s).
- A PC with an Ethernet NIC for configuring basic parameters of the WiFi AP and the SU-ODU, and a b/g WiFi card for testing wireless connectivity to the AP.
- Wall - Tilt Pole Mounting kit* ([page 28](#))
- DC power connector* (pack of 5)
- Waterproof covers for AC/DC socket* (pack of 5)

NOTE

Before starting to install the Wi² unit, check that you have all the necessary parts and accessories. Optional accessories marked with an asterisk (*) can be ordered from your supplier.

2.2.3 Guidelines for Positioning Wi²

CAUTION



ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

Failure to do so may void the product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

The Wi² should be mounted vertically on a 2"- 6" pole. Its location should enable easy access to the unit and its connectors for installation and maintenance and should have a clear or near line of sight to the area to be covered.

For best performance, the SU-ODU attached to the unit should have clear or near line of sight to the base station. For further information about the optimal installation location of the SU-ODU refer to the relevant manual.

2.3 Installation

The following sections describe how to install a Wi² unit, including attaching the SU-ODU to the mounting plate, attaching the mounting plate to the Wi² unit, connecting to the SU-ODU, pole mounting, connecting a grounding cable, and connecting the antenna(s).

2.3.1 Attaching the SU-ODU to the Mounting Plate

IMPORTANT



The angle at which the SU-ODU is mounted on the Wi² can be adapted depending on the location of the Wi² unit in relation to the Base Station. Once attached, the mounting plate can be tilted either up or down. Before attaching the SU-ODU to the mounting plate, determine the direction of the tilt.



To attach a BreezeMAX PRO-S ODU or BreezeACCESSSU-ODU with HW Revision E (octagonal) to the mounting plate:

NOTE



BreezeACCESS SU-ODU with HW Revision E is the new, smaller, octagonal ODU available in the 5.4 and 5.8 GHz bands. BreezeACCESS SU-ODUs with HW Revision D or lower are rectangular and slightly larger in size.

- 1 Determine the tilt direction of the SU-ODU.
- 2 Using the M8 x 16 hex head screws and the flat washers and spring washers supplied, attach the SU-ODU to the mounting plate as shown in [Figure 2-5](#) in the direction marked.
- 3 Tighten the screws. Apply torque of 57 lb*in [6.4 N*m].

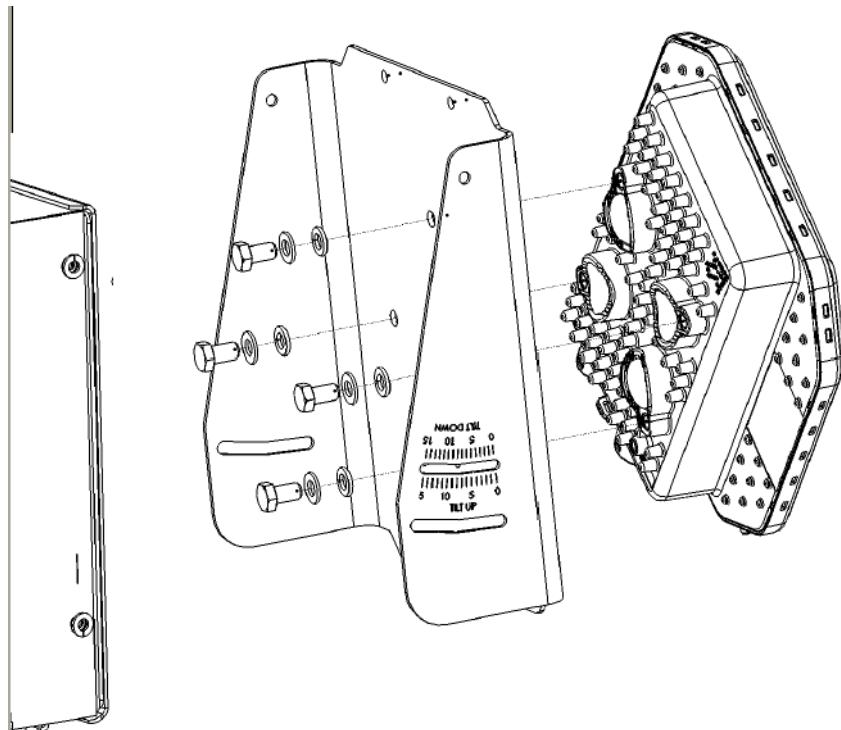


Figure 2-5: Attaching BreezeMAX PRO-S ODU or BreezeACCESSSU-ODU with HW Revision E to Mounting Plate

NOTE



For information about polarization refer to the relevant manual.



To attach a BreezeACCESS SU-ODU with HW Revision D or lower (rectangular) to the mounting plate:

- 1** Determine the tilt direction of the SU-ODU.
- 2** Using the 1/4" x 1/2" hex head screws and the flat washers and spring washers supplied, attach the SU-ODU to the mounting plate as shown in [Figure 2-6](#) in the direction marked.
- 3** Tighten the screws. Apply torque of 57 lb*in [6.4 N*m].

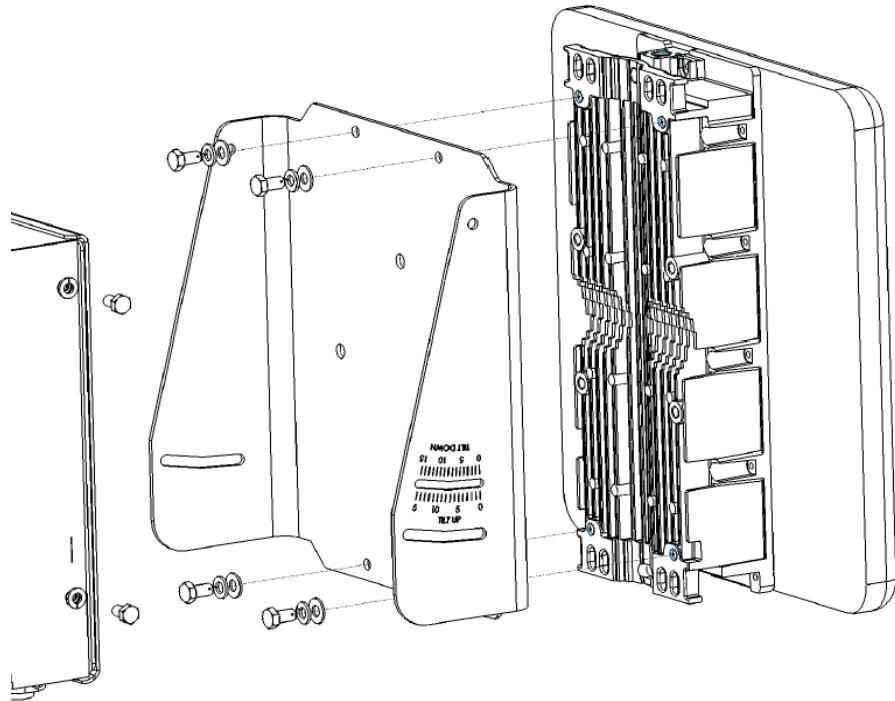


Figure 2-6: Attaching BreezeACCESS SU-ODU with HW Revision D or lower to Mounting Plate

NOTE



Sometimes, physical circumstance require that the SU-ODU be located at a distance from the Wi² unit and not attached to the mounting plate. For further information see the section on SU-ODU mounting in the relevant manual.

2.3.2 Attaching the Mounting Plate to the Wi² Unit

- 1 Hold the mounting plate with SU-ODU attached so the tilt label faces the tilt direction that you have decided upon (see [Section 2.3.1](#)).
- 2 Using the M6 x 12 hex head screws and the flat washers and spring washers supplied, attach the mounting plate to the Wi² unit as shown in [Figure 2-7](#).

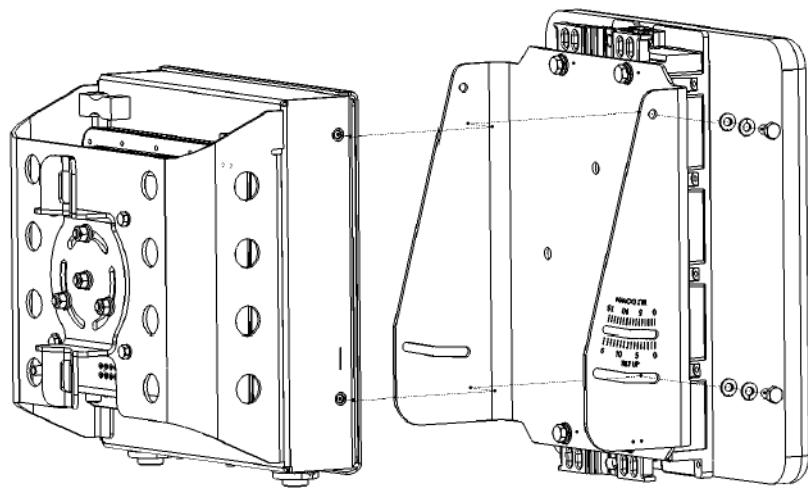


Figure 2-7: Attaching the Mounting Plate to the Wi² Unit

- 3 Adjust the tilt angle according to the scale marked on the mounting plate and tighten the screws. Apply torque of 57 lb*in [6.4 N*m].

2.3.3 Connecting the Wi² Unit to the SU-ODU

NOTE



The Wi² installation kit includes a Category 5E Ethernet cable, suitable for connecting to BreezeMAX PRO-S ODU. For instructions on how to adapt the Ethernet cable for connecting to a BreezeACCESS SU-ODU with HW revision D or lower refer to [“Section 2.3.3.2, “Adapting the Ethernet Cable for Connecting to BreezeACCESS SU-ODU” on page 2-24](#)

2.3.3.1 Connecting to BreezeMAX PRO-S ODU

- 1 The rubber sealing cap (supplied with the SU-ODU) has a special groove allowing to insert an ethernet cable with an already assembled RJ-45 connector through the cap. To expose the groove, lightly squeeze the cap (see [Figure 2-8](#)). Carefully insert the end of the 55 cm category 5E Ethernet cable without the service box through the groove.

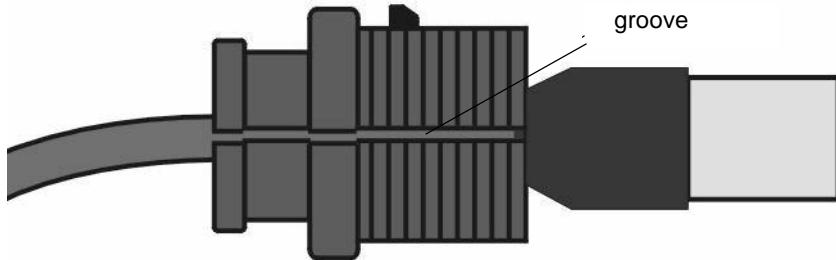


Figure 2-8: Sealing Cap

- 2 Expose the RJ-45 connector under the sealing cap on the Ethernet cable and connect to the SU-ODU RJ-45 connector ([Figure 2-9](#)).

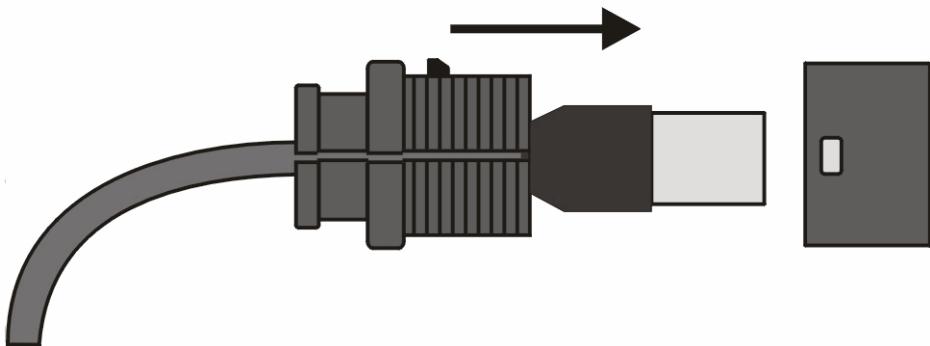


Figure 2-9: Connecting the SU-ODU connector and inserting the Sealing Cap

- 3 Put the sealing cap back in its place. Make sure that the small protrusion on the side of the cap fits inside the hole on the connector's protective body.
- 4 Connect the other end of the Ethernet cable to the SU port on the Wi² unit.
- 5 Verify that the O-ring supplied with the service box kit is in place, attach the service box to the unit and tighten the top nut.
- 6 Use appropriate sealing material to protect the connection to the SU-ODU against moisture and humidity. Use removable sealing material to enable future access to the connector.

NOTE



Use high quality sealing material such as Scotch® 130C Linerless Rubber Splicing Tape from 3M to ensure IP-67 compliant protection against dust and water.

2.3.3.2 Adapting the Ethernet Cable for Connecting to BreezeACCESS SU-ODU

The 55 cm Ethernet cable supplied with the unit has crossed Ethernet connections which have to be adapted for connecting the unit to a BreezeACCESS ODU:

- 1 Cut the cable as close as possible to the connector that should be connected to the ODU (the end without the service box).
- 2 Use a crimp tool for RJ-45 connectors to prepare the wires. Insert them into the appropriate pins of the spare RJ-45 connector supplied with the unit and use the tool to crimp the connector. Make sure to do the following:
 - » Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the sealing cover when connected to the unit, to ensure good sealing.
 - » Pull back the shield drain wire before inserting the cable into the RJ-45 connector, to ensure a good connection with the connector's shield after crimping.

The cable should provide straight pin-to-pin connections on both ends.

[Figure 2-10](#) shows the required wire pair connections:

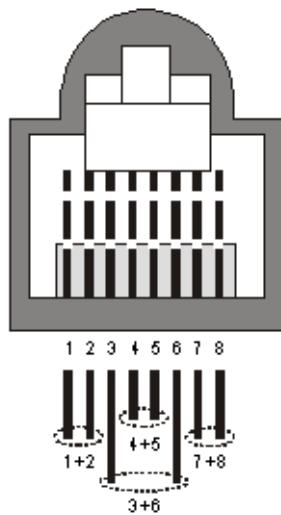


Figure 2-10: Ethernet Connector Pin Assignments

The color codes used in the standard cable supplied by with the unit are listed in the table below.

Wire color	Pin
Blue	1
Blue/white	2
Orange	3
Orange/white	6
Brown	4
Brown/white	5
Green	7
Green/white	8

2.3.3.3 Connecting to BreezeACCESS ODU with HW Revision E

- 1 Adapt the cable as described in [Section 2.3.3.2](#)
- 2 Connect the cable to the ODU as described in [Section 2.3.3.1](#).

2.3.3.4 Connecting to BreezeACCESS ODU with HW Revision D or Lower

- 1 Cut the cable as close as possible to the connector that should be connected to the ODU (the end without the service box).
- 2 Route the cable through the service box supplied with the SU-ODU.
- 3 Connect the spare RJ-45 connector, supplied with the cable kit, as described in step 2 of [Section 2.3.3.2](#)
- 4 Connect the Ethernet cable to the SU-ODU RJ-45 connector.
- 5 Make sure that the external jacket of the cable is well inside the service box to guarantee a good seal.
- 6 Verify that the O-ring of the service box kit is in place, attach the service box to the unit and tighten the top nut.
- 7 Connect the other end of the cable to the SU port on the Wi² unit.
- 8 Make sure that the external jacket of the cable is well inside the service box to guarantee a good seal. Verify that the O-ring supplied with the service box is in place, attach the service box to the unit and tighten the top nut.

2.3.4 Preparing the Power Cable

CAUTION



Electric Shock Hazard. Only a licensed electrician should connect the power plug.

All mains used outdoors, in damp or wet conditions, should be supplied from a correctly fused source and protected according to applicable local regulations.



To prepare the power cable:

- 1 Use a UL/CSA listed smooth circular power cable, 1.5mm to 2.5mm each. Outer diameter 7mm to 9mm, UV resistant, temperature range -40°C to + 65°C (-40°F to +149°F) minimum. Other specifications (such as oil resistance, no of wires) according to specific installation requirements.
- 2 Use a cap assembly tool to unscrew the locking ring.
- 3 Thread the cable through component parts as shown in [Figure 2-11](#).

NOTE



[Figure 2-11](#) shows an AC power jack. The DC power jack is similar, but has only two sockets.

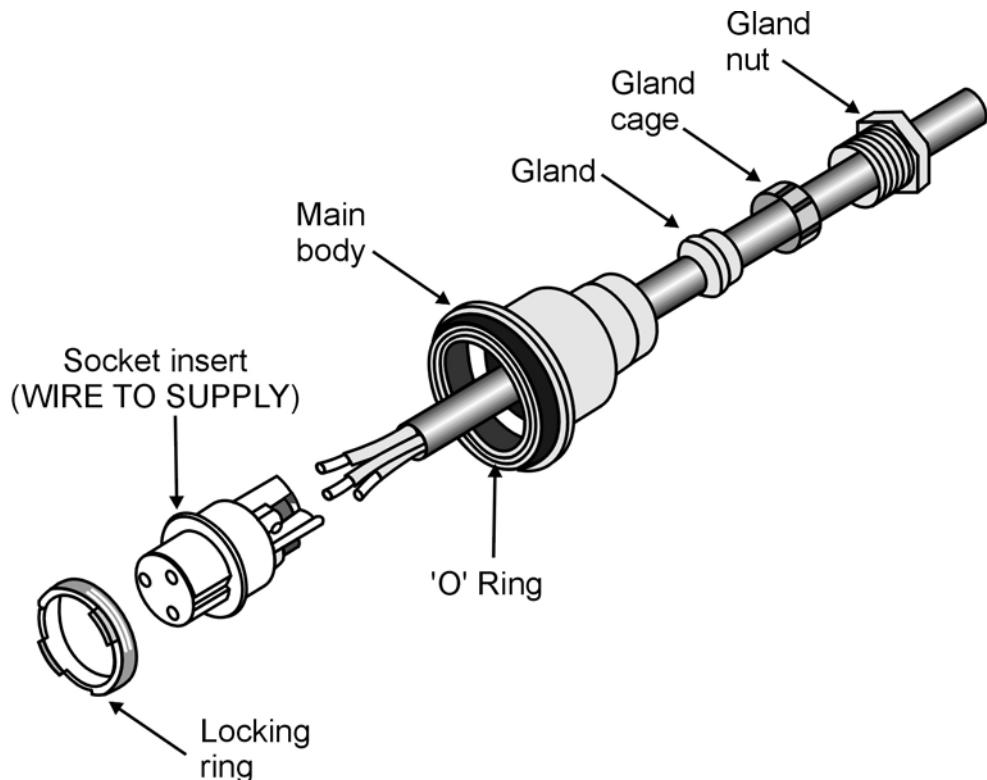


Figure 2-11: Preparing the Power Cable

- 4 Strip insulation from wires as shown in [Figure 2-11](#).
- 5 Insert bare wire ends into the terminals and fully tighten the screws. The wires should be connected as shown below:

AC		DC	
Brown	Phase ~	Red	+
Blue	Neutral 0	Black	-
Yellow/green	Grounding		

- 6 Draw cable back until socket insert is correctly seated in D-shaped location in the main body. Tighten the Gland nut. Screw back the locking ring using the cap assembly tool.
- 7 For an AC cable, connect a mains plug to the other end of the cable. For a DC cable, connect the appropriate termination.

2.3.5 Mounting the Wi² Unit



To pole mount the Wi² unit:

- 1 With the bottom panel of the unit facing downwards, thread the two 9/16" wide metal bands supplied through the brackets on the sides of the unit.
- 2 Rotate the mounting bracket, so that the Wi² faces the Base Station.

NOTE



The mounting bracket can be rotated up to 45° in any direction.

- 3 Secure the Wi² unit to a pole as shown in [Figure 2-12](#).

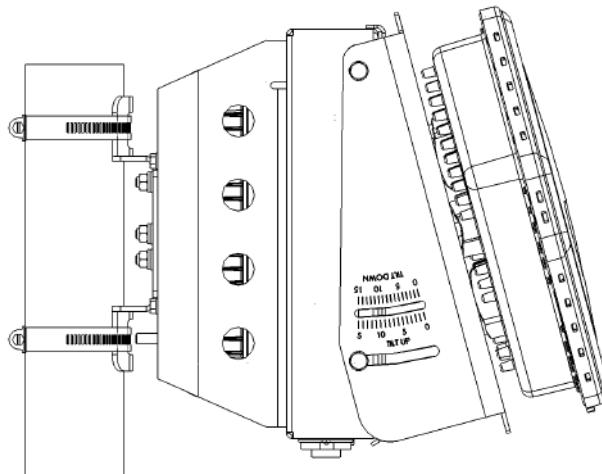


Figure 2-12: Pole Mounting the Wi²

2.3.5.1 Mounting the Wi² Using the Tilt Accessory

The Wi² can also be installed on a wall or on a non-vertical pole using an optional tilt accessory kit. The tilt accessory kit ([Figure 2-13](#)) includes:

- A mounting bracket
- 3 metal bands for attaching the bracket to a pole
- Screws for attaching the bracket to a wall

- A 50 cm pole (diameter 6.03 cm)
- Screws for attaching the pole to mounting bracket

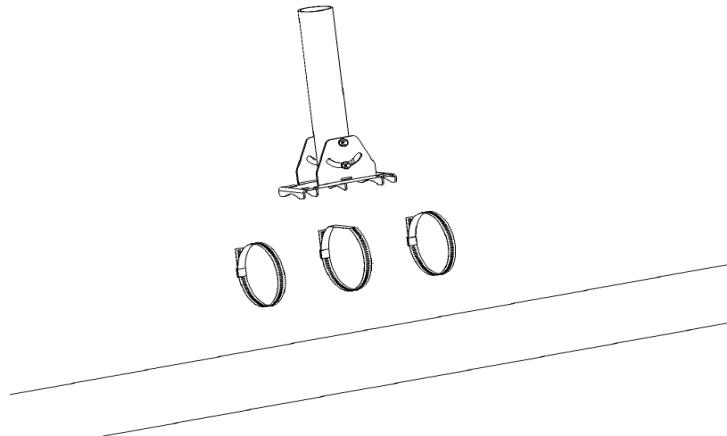


Figure 2-13: Tilt Accessory Kit



To mount the tilt accessory on a wall:

- 1 Place the bracket on the wall and use as a template to mark the position of the holes to be drilled for the screws .
- 2 Remove the bracket from the wall and drill a hole in each of the locations marked.
- 3 Insert anchors into the holes.
- 4 Hold the bracket over the holes and insert a screw into each of the holes in the bracket, and screw into the anchors in the wall. Secure the bracket to the wall, making sure that the screw heads are as level with the bracket as possible.



To mount the tilt accessory on a non-vertical pole:

- Thread the metal bands provided with the tilt accessory through the slits in the bracket and attach to the pole as shown in [Figure 2-14](#).

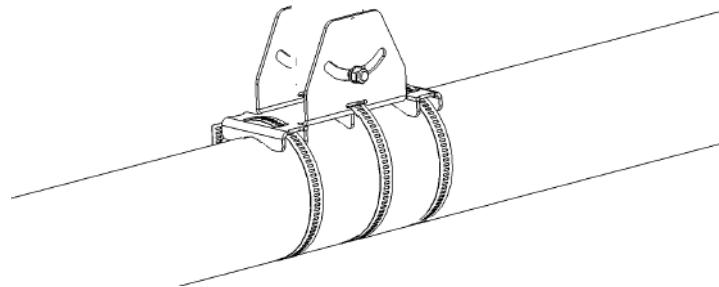


Figure 2-14: Mounting Tilt Accessory on Non-Vertical Pole



To mount the Wi² using the tilt accessory:

- 1 Mount the tilt accessory bracket on the wall or pole as described above.
- 2 Using the screws provided attach the pole to the tilt accessory bracket.
- 3 Using a spirit level, adjust the angle of the pole until it is vertical and tighten the screws to hold in place.
- 4 Secure the Wi² to the pole as described in “Mounting the Wi² Unit” on page 28.

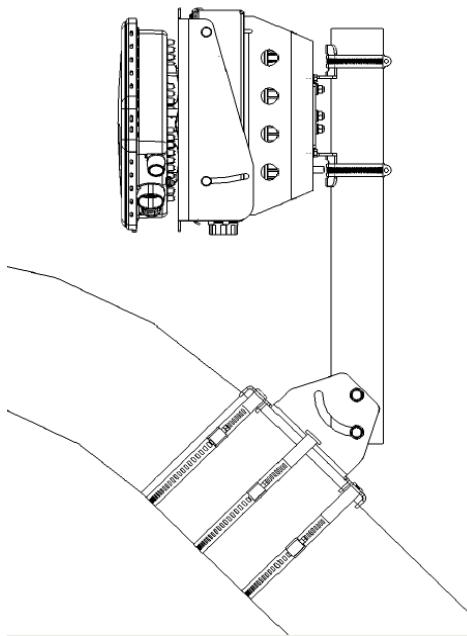


Figure 2-15: Wi² Mounting Using the Tilt Accessory

2.3.6 Connecting the Antenna(s)



To connect an external antenna:

- 1 Connect the external antenna directly to the N-type connector on the top panel of the Wi² unit.

NOTE



When connecting only one antenna, connect it to the right antenna connector. (When looking at the unit from the side of the SU-ODU with the antenna connectors facing upwards, this is the connector on the right.)

- 2 Set the antenna options for corresponding antenna through the user interface (refer to the *AP CLI Reference Guide*).

CAUTION



If using antennas other than the Omni 8, make sure you do not exceed local radio regulations.

2.3.7 Connecting the Grounding Cables



To connect the grounding cables:

- 1 Connect a grounding cable to the grounding stud on the Wi² unit and tighten the grounding screw firmly.
- 2 Connect a grounding cable to the grounding stud on the SU-ODU and tighten the grounding screw firmly.
- 3 Connect the other ends of the grounding cables to a good ground (earth) connection.

CAUTION



Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.

2.3.8 Connecting to Power Source

- 1 Connect the power cable (see Section 2.3.4) to the power socket on the unit and to the mains supply.

CAUTION

The Wi² can be connected to either an AC or DC power source, or to both. By default the DC plug is covered with a waterproof sealing cap which must be removed before connecting to the power cable. Any socket that is NOT in use must always be protected from moisture and must be covered with a waterproof sealing cap.

- 2 Check that the LED on the Wi² is green indicating that the system is working normally.

2.3.9 Configuration and Testing

2.3.9.1 Configuring the SU-ODU

- 1 Disconnect the cable connecting the WiFi Access Point (AP) from the AP connector on the Power Supply and Interface module.
- 2 Connect a PC to the AP connector using the 3 m configuration cable (straight) supplied with the unit.
- 3 Verify that the SU-ODU is connected to the SU connector on the Power Supply and Interface module.
- 4 Using Telnet, connect to the SU-ODU and configure its parameters. For configuration details refer to the relevant manual.
- 5 Verify that the SU-ODU is operating properly and that it connects to the base station. For details on verifying proper operation and connectivity refer to the relevant manual.

2.3.9.2 Configuring the Wi²

- 1 Disconnect the configuration cable from the unit and reconnect the cable between the WiFi Access Point (AP) and the AP connector of the Power Supply and Interface module.
- 2 Disconnect the cable connected to the SU connector on the Power Supply and Interface module.
- 3 Connect a PC to the SU connector using the 3 m configuration cable.

NOTE

Alternatively, instead of disconnecting the SU connector, you can connect a PC to the Console port of the AP with a console cable (ordered separately) and complete all the configuration using CLI.

- 4 Using SSH or web, log in, and set the country code (available only via CLI) and the AP IP address as outlined in [Chapter 4 - "Getting Started"](#).

- 5 Complete the configuration of the AP, using either CLI as outlined in the *AP CLI Reference Guide* or the web-based interface as outlined in [Chapter 8](#).

NOTE



At least one VAP must be enabled and Antenna ID must be configured to enable transmissions.

- 6 Disconnect the configuration cable from the Wi² unit and reconnect the cable between the SU-ODU and the SU connector of the Power Supply and Interface module.
- 7 Using the WiFi client (802.11b/g), locate the Wi² and verify complete connectivity to the backbone network.



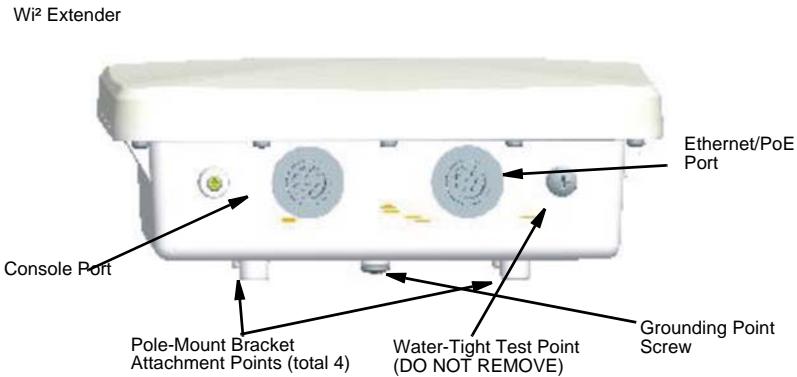
3

Chapter 3 - Hardware Installation Wi² Extender

In This Chapter:

- “Wi² Extender ODU Hardware Description” on page 36
- “Installation Requirements” on page 38
- “Mounting the Wi² Extender ODU” on page 40
- “Connecting Cables to the Outdoor Unit” on page 45
- “The Power Injector IDU” on page 46
- “Connecting the Power Injector IDU Cables” on page 47

3.1 Wi² Extender ODU Hardware Description



3.1.1 Ethernet Port

The Wi² Extender ODU has one 10BASE-T/100BASE-TX RJ-45 port that connects to the power injector IDU using an Ethernet cable. The Ethernet port connection provides power to the Wi² Extender as well as a data link to the local network via the IDU.

The unit appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to the remote Access Unit.

3.1.2 Console Port

The Wi² Extender has a console port for connecting to the command line interface.

3.1.3 Grounding Point

Even though the Wi² Extender includes its own built-in lightning protection, it is important that the unit is properly connected to ground. A grounding screw is provided for attaching a ground wire to the unit.

3.1.4 Water Tight Test Point

CAUTION



Do not remove or loosen this screw. Doing so could lead to damage of the unit.

3.1.5 Pole-Mounting Bracket Attachment Points

The Wi² Extender includes a bracket kit that can be used to mount the unit to a pole, radio mast, or part of a tower structure.

3.1.6 LED Indicators

The Wi² Extender includes status LED indicators located on the base of the unit, as indicated in the following figure.

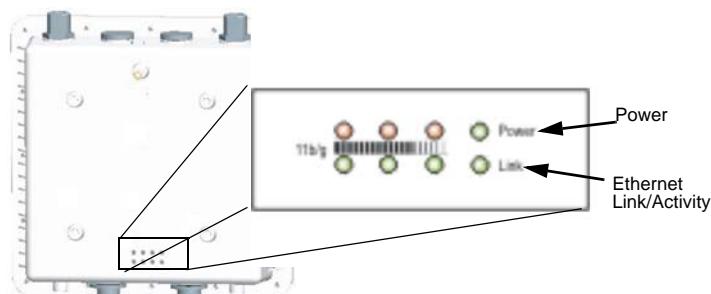


Figure 3-1: LEDs

The following table describes the system status LEDs::

LED	Status	Description
Power	On Green	Indicates that the system is working normally.
	On Amber	Indicates a system reset.
Link	On Green	Indicates a valid 10/100 Mbps Ethernet cable link.
	Flashing Green	Indicates that the Wi ² Extender is transmitting or receiving data on a 10/100 Mbps Ethernet LAN. Flashing rate is proportional to network activity.

Once the AP has established a secure tunnel with a CTRL, the status lights revert to their normal operation:

- Power light is solid to indicate that the AP is fully operational
- Ethernet light blinks to indicate the presence of traffic on the Ethernet port
- Wireless light blinks to indicate the presence of traffic on the wireless port

3.2 Installation Requirements

This section describes all the supplies required to install the Wi² Extender and the items included in each installation package.

3.2.1 Packing List

The Wi² Extender package includes the following components:

- Wi² Extender
- A pole mounting kit for the Wi² Extender, including a mounting plate and a metal band and four screws
- Mains power cord EU
- Mains power cord US
- IDU power supply
- This Product Manual with CD and Quick Installation Guide.

Additional items required for installation:

- Category 5E cable (PoE) length 30m (ordered separately)

3.2.2 Additional/Optional Installation Requirements

- RS232 console cable*
- 8 dBi Omnidirectional antenna(s)*
- Sectoral antenna(s), including RF cable with N-Type connector*
- Grounding cable with an appropriate termination.
- Installation tools and materials, including appropriate means for installing the Wi² Extender and antenna(s).
- A PC with an Ethernet NIC for configuring basic parameters of the WiFi AP, and a b/g WiFi card for testing wireless connectivity to the AP.
- 3M Scotch tape and natural rubber to isolate the antenna and PoE port from humidity

NOTE



Before starting to install the Wi² Extender unit, check that you have all the necessary parts and accessories. Optional accessories marked with an asterisk (*) can be ordered from your supplier.

3.2.3 Guidelines for Positioning Wi² Extender

CAUTION



ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

Failure to do so may void the product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

The Wi² Extender should be mounted vertically on a 2"- 6" pole. Its location should enable easy access to the unit and its connectors for installation and maintenance and should have a clear or near line of sight to the area to be covered.

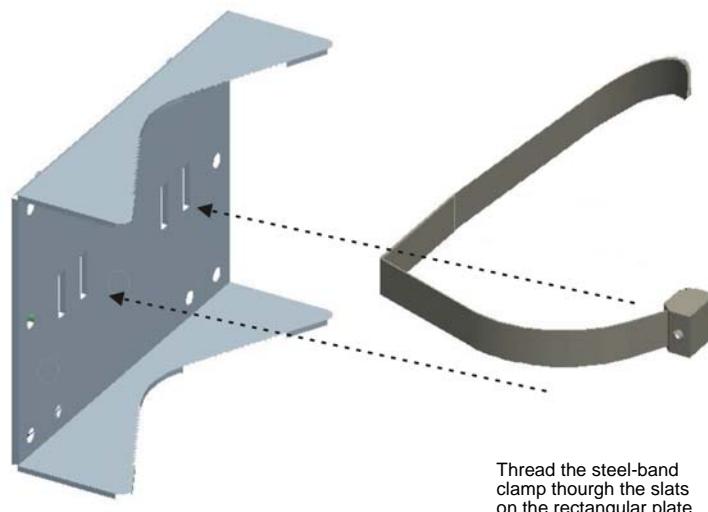
For best performance, the Wi² Extender attached to the unit should have clear or near line of sight to the base station. For further information about the optimal installation location of the Wi² Extender, refer to the relevant manual.

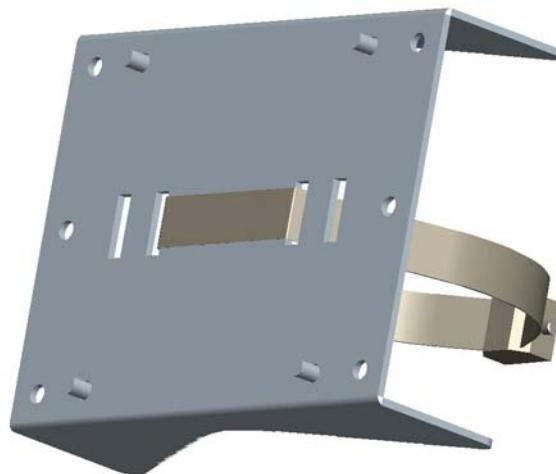
3.3 Mounting the Wi² Extender ODU

The Wi² Extender's pole-mounting bracket has two parts: One rectangular plate with V-shaped edges that attaches directly to the Wi² Extender ODU, and one steel-band clamp that secures the unit to a pole. The rectangular plate connects to the unit using four screws. The steel-band clamp threads through the rectangular plate and around the pole to which it fastens.

Perform the following steps to mount the unit to a 1.5 to 2 inch diameter steel pole or tube using the mounting bracket:

- 1 Thread the provided steel-band through the rectangular plate.





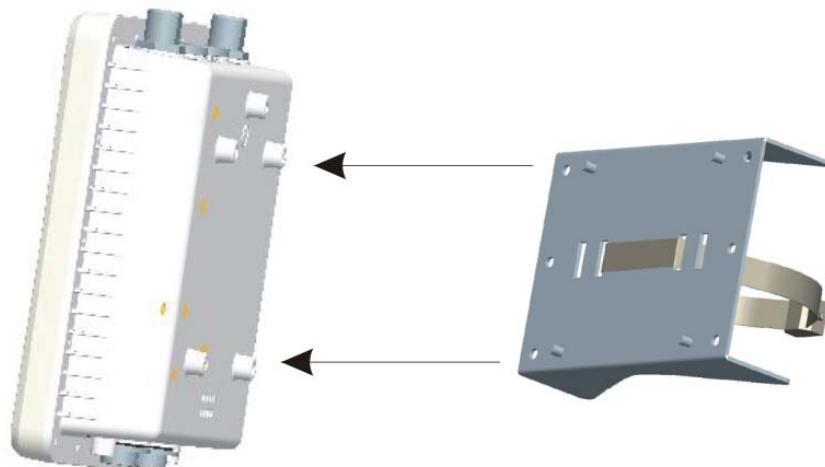
- 2** Attach the rectangular mounting plate to the Wi² Extender using the supplied four screws.

NOTE

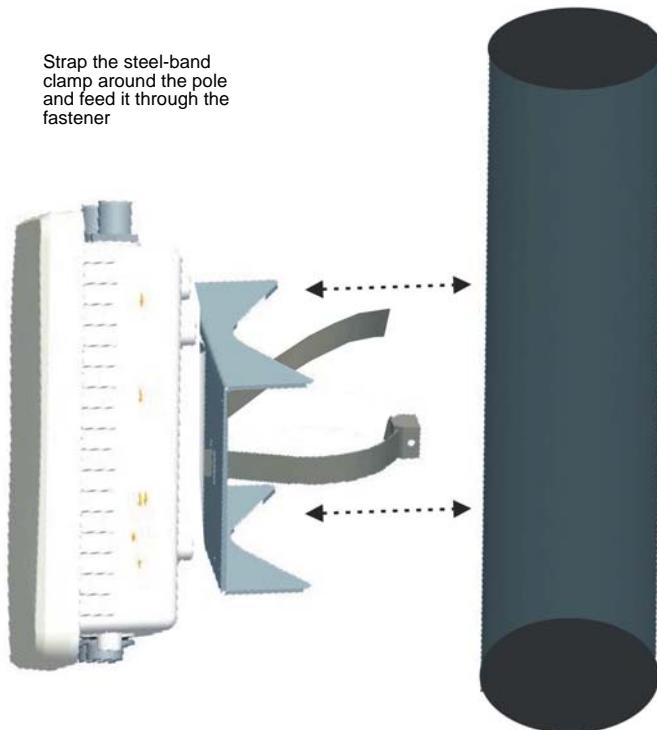


The mounting plate can be attached to the unit in a way that allows it to be mounted vertically or at a 45 degree angle.

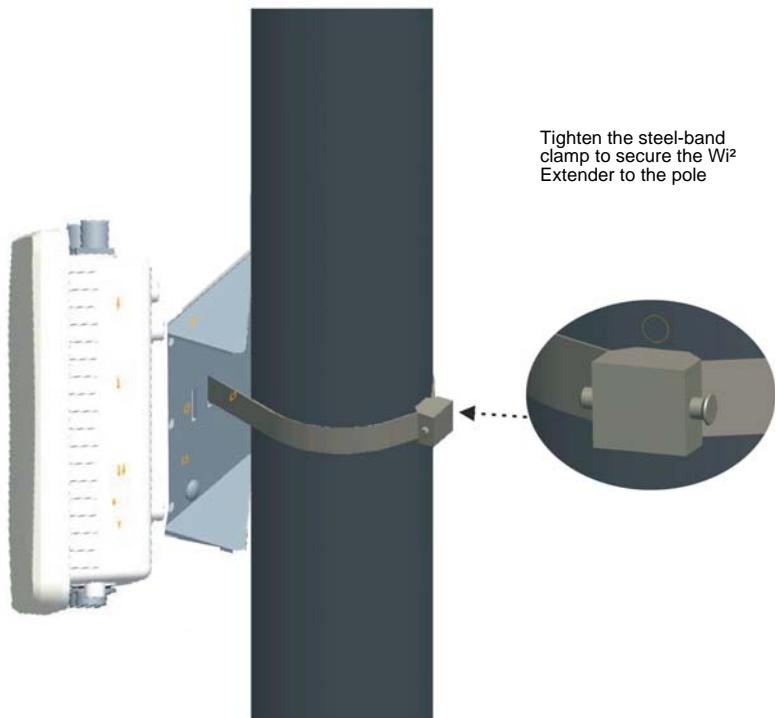
Secure the rectangular
Wi² Extender using the
supplied screws



- 3 Place the Wi² Extender with its attached rectangular plate on one side of the pole and strap the steel-band clamp around the pole. Feed the steel band through its fastener and secure it tightly.

**NOTE**

Be sure to take account of the antenna polarization direction; antennas in a link must be mounted with the same polarization.



3.4 Connecting Cables to the Outdoor Unit

WARNING



Do not connect or disconnect cables or otherwise work with the Wi² Extender during periods of lightning activity.

3.4.1 Grounding Wire

Be sure to ground the Outdoor Unit with an appropriate grounding wire (not included) by connecting the grounding point on the base of the unit to a good ground (earth) connection.

CAUTION



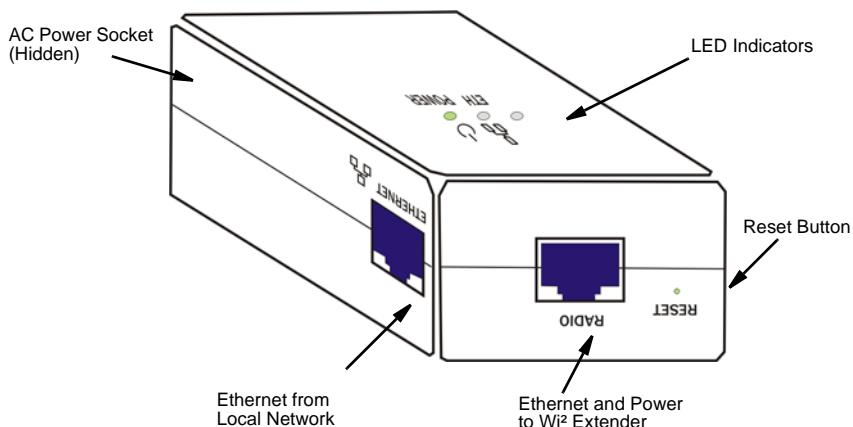
Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.



3.5 The Power Injector IDU

The Wi² Extender receives power through its network cable connection using power-over-Ethernet technology. A power injector IDU is included in the Wi² Extender package and provides two RJ-45 Ethernet ports, one for connecting to the Wi² Extender (Radio), and the other for connecting to a local LAN switch (Ethernet).

The Ethernet port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports. However, when connecting the Wi² Extender to a workstation or other device that does not have MDI-X ports, you must use a crossover twisted-pair cable.



The Wi² Extender does not have a power switch. It is powered on when its Ethernet port is connected to the power injector module, and the power injector module is connected to an AC power source.

The Power LED indicates whether AC power is applied. The Link LED does not function in current release of Wi² Extender.

In the current release, the Reset button does not function.

The power injector module automatically adjusts to any AC voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

WARNING



The power injector module is designed for indoor use only. Never mount the power injector outside with the Wi² Extender unit.

3.6 Connecting the Power Injector IDU Cables

The unit can be placed on a desktop or a shelf. Alternatively, it may be wall-mounted using the kit supplied with the unit.

CAUTION



Do not install the power injector outdoors. The unit is for indoor installation only.

CAUTION



Install lightning protection at the power injector end of the Ethernet cable, use a lightning arrestor immediately before the cable enters the building.

NOTE



The Wi² Extender's Ethernet port does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. Do not try to power the unit by connecting it directly to a network switch that provides IEEE 802.3af PoE. Always connect the unit to the included power injector module.



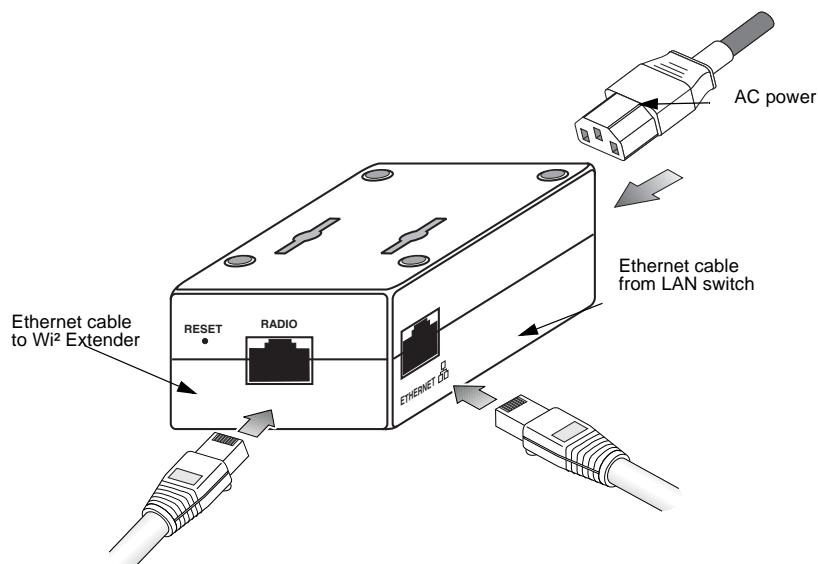
To connect the IDU cables:

- 1 Connect the Ethernet cable from the Wi² Extender ODU to the RJ-45 port labeled “Radio” on the power injector IDU.
- 2 Connect a straight-through unshielded twisted-pair (UTP) cable from a local LAN switch/router to the RJ-45 port labeled “Ethernet” on the power injector. If you connect to a workstation, use a crossover cable. Use Category 5E or better UTP cable for 10/100BASE-TX connections.

NOTE



The RJ-45 port on the power injector is an MDI port. If connecting directly to a computer, use a crossover cable.



- 3 Insert the power cable plug directly into the standard AC receptacle on the power injector.
- 4 Plug the other end of the power cable into a grounded, 3-pin socket, AC power source.

NOTE



For International use, you may need to change the AC line cord. You must use a line cord set that has been approved for the receptacle type in your country.

- 5 Check the Power LED on top of the power injector IDU to be sure that power is being supplied to it.

3.6.1 Connecting the Antenna(s)



To connect an external antenna:

- 1 Connect the external antenna directly to the N-type connector on the top panel of the Wi² Extender unit.

NOTE



When connecting only one antenna, connect it to the right antenna connector. (When looking at the unit from the side of the Wi² Extender with the antenna connectors facing upwards, this is the connector on the right.)

- 2 Set the antenna options for corresponding antenna through the user interface (refer to the *AP CLI Reference Guide*).

CAUTION

If using antennas other than the Omni 8, make sure you do not exceed local radio regulations.

3.6.2 Connecting the Grounding Cables

**To connect the grounding cables:**

- 1 Connect a grounding cable to the grounding stud on the Wi² Extender unit and tighten the grounding screw firmly.
- 2 Connect a grounding cable to the grounding stud on the Wi² Extender and tighten the grounding screw firmly.
- 3 Connect the other ends of the grounding cables to a good ground (earth) connection.

CAUTION

Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.

3.6.3 Connecting to Power Source

- 1 Connect the PoE cable to the Ethernet port on the power supply and make sure the power supply is connected to a mains source.
- 2 Connect the other end of the Ethernet cable to the Wi² Extender.
- 3 Check that the LED on the Wi² Extender is green indicating that the system is working normally.

3.6.4 Configuration and Testing

- 1 Connect a PC to the Ethernet port of the IDU connector using a crossover cable.

NOTE

Alternatively you can connect a PC to the Console port of the AP with a console cable (ordered separately) and complete all the configuration using CLI.

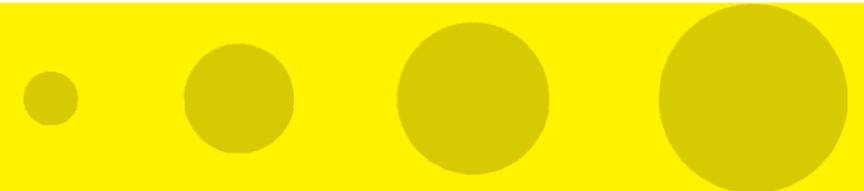
- 2** Using SSH or web, log in, and set the country code and the AP IP address as outlined in [Chapter 4 - "Getting Started"](#).
- 3** Complete the configuration of the AP, using either CLI as outlined in the *AP CLI Reference Guide* or the web-based interface as outlined in [Chapter 8](#).

NOTE



At least one VAP must be enabled and Antenna ID must be configured to enable transmissions.

- 4** Disconnect the configuration cable from the Wi² Extender unit.
- 5** Using the WiFi client (802.11b/g), locate the Wi² Extender and verify complete connectivity to the backbone network.



4

Chapter 4 - Getting Started

In This Chapter:

- “Introduction” on page 52
- “Configuration Procedure” on page 53

4.1 Introduction

This chapter walks you through the steps needed to initially configure the AP in autonomous mode and establish a connection through the AP to the Internet.

If you are using the AP in its default controlled mode in which it is managed by an Wi² series service controller, see a *Wi² Series Quickstart* and “*Working with controlled APs*” in the *Wi² Series Admin Guide*.

Although the screen images here are taken from the Wi² AP, the procedures apply equally to the Wi² AP series, with variations for the ruggedized versions (Wi² AP) noted where they occur. In the management tool for ruggedized versions, ignore any references to Port 2.

4.2 Configuration Procedure

This section walks you through the steps needed to configure the service controller and establish a connection through the service controller to the Internet.

The service controller is managed via its web-based management tool using at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0.

NOTE



Do not power on Alvarion Ltd. hardware until directed.

CAUTION



WIRELESS SECURITY: To provide easy wireless access to the management interface, the AP ships with all wireless security options disabled. Alvarion strongly recommends that once the AP is installed, you enable a wireless security option to properly safeguard the wireless network from intruders.



To configure your computer

- 1 Connect the Ethernet port on your computer to Ethernet port 1 on the AP.
- 2 Configure your computer to use a static IP address in the range **192.168.1.2** to **192.168.1.254**. The subnet mask of **255.255.255.0** is entered automatically. Set the default gateway to **192.168.1.1**, and DNS server to **192.168.1.1**

For example, in Windows XP, use **Control Panel > Network Connections > Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties**.

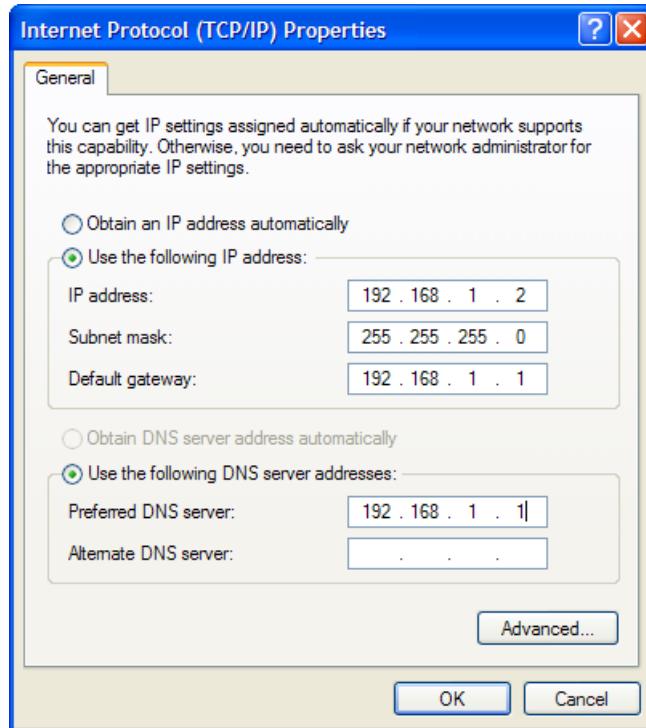


Figure 4-1: TCP/IP Properties Window

- 3 Disable any wireless connection.

To start the AP



Connect the power supply (sold separately) or use a PoE injector to power-up the AP.

Ruggedized version: Connect the PoE injector to power-up the AP.

To perform these initial login tasks



- 1 In a web browser, open page: **https://192.168.1.1**.
- 2 You are prompted to accept a security certificate. To continue, proceed as follows: At the security certificate prompt, in Internet Explorer 7, select **Continue to this website**.

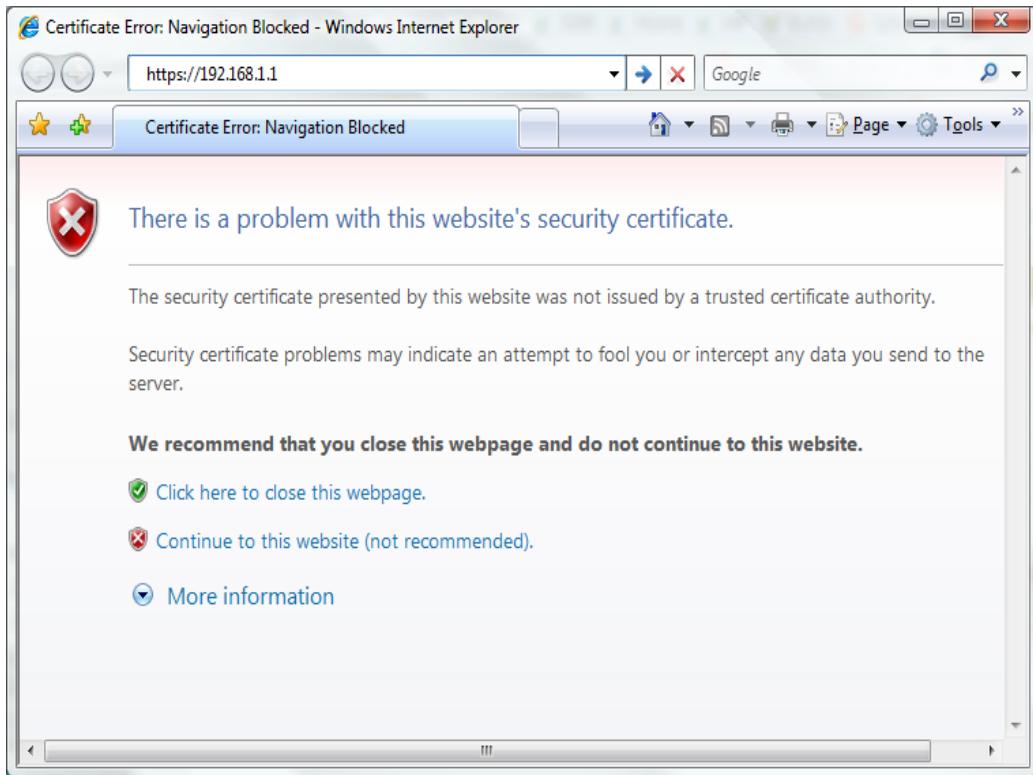


Figure 4-2: Windows Security Message

In Firefox 2, select select **Accept this certificate temporarily for this session** and then **OK**.



Figure 4-3: Certificate Window

For information on how you can replace the Secure Sockets Layer (SSL) certificate that ships with the AP with one of your own, see “[Managing Certificates](#)” on page 155.

- 3 On the Login page, specify **admin** for **Username** and **Password** and then select **Login**. The AP management tool home page opens.
- 4 Select the **Switch to Autonomous Mode** button and confirm the change. The AP management tool restarts within a few minutes.

To perform the initial autonomous login

- 1 On the Login page, specify **admin** for **Username** and **Password** and then select **Login**.
- 2 On the License Agreement page, read the agreement and select **Accept License Agreement**.
- 3 On the registration page, select **Register Later**. You can register by selecting **Maintenance > Registration**.

- 4 If presented with a **Country** prompt, choose the country in which this product will be used and select **Save**.
- 5 At the password prompt it is recommended that you change the password. Specify the new password and select **Save**. The management tool home page opens.

NOTE



Instructions to select specific elements and menus are specified in the form:
Select **Network > Ports**. This instructs you to select the **Network** main menu, and its **Ports** sub-menu.

Key elements of the management tool user interface are defined as follows:

The screenshot shows the management tool's main interface. At the top, there is a navigation bar with tabs: VSC, Wireless, Network, Security, Management, Status, Tools, and Maintenance. The 'Network' tab is selected. Below the navigation bar, there is a sub-menu bar with tabs: Ports, Bandwidth control, CDP, DNS, IP routes, and IP QoS. The 'Ports' tab is selected. To the right of the sub-menu bar, two arrows point to the text: 'Main Menu' points to the 'Management' tab in the top bar, and 'Sub-menu' points to the 'Ports' tab in the bottom bar. Below the sub-menu bar, there are two tables. The first table is titled 'Port configuration' and lists three ports: 'Bridge port' (IP address 192.168.1.55, Mask 255.255.255.0, MAC address 00:10:E7:02:42:E0), 'Wireless port' (IP address [bridged], Mask [bridged], MAC address 00:10:E7:02:42:E0), and 'Port 1' (IP address [bridged], Mask [bridged], MAC address 00:10:E7:02:48:CC). The second table is titled 'VLAN configuration' and has columns: Name, Port, VLAN, IP address, and Mask. It contains one row with a 'Name' column entry and a 'Add New VLAN...' button.

Figure 4-4: Main Page



To test the wireless network

By default, the AP operates as a DHCP client to obtain its IP address from a DHCP server.

- 1 Remove the cable and connect the AP with a standard Ethernet cable to the network on which it will be used. The network must have a DHCP server and an Internet connection. Broadband routers typically include a DHCP server.

Ruggedized version: Remove the crossover cable, and using a standard Ethernet cable connect the PoE injector **Data In** port to the network on which the AP will be used. The network must have a DHCP server and an Internet connection. Broadband routers typically include a DHCP server.

- 2 Enable your computer's wireless network interface, and verify that it is set to obtain an IP address automatically.

For example, in Windows XP, use **Control Panel > Network Connections > Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties**, and make sure that **Obtain an IP address automatically** and **Obtain a DNS server address automatically** are both checked.

- 3 Connect to the wireless network. For example, from the Windows XP Start menu, select **Settings > Network Connections > Wireless Network Connections**. The list of available wireless networks appears. By default the AP creates a wireless network named *Alvarion Ltd.*. Select this network and then **Connect**.

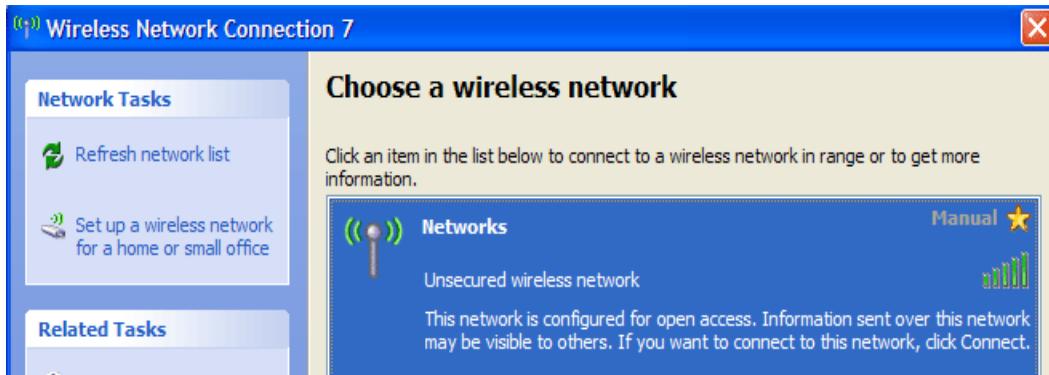


Figure 4-5: Choosing a Wireless Network

- 4 Confirm that you can browse the Internet using the wireless network.



To perform additional configuration

- 1 Make sure that your computer is configured to obtain an IP address and DNS Server address automatically, as in step E. 2 above.
- 2 Connect your computer to the same network as the AP.
- 3 Look in the DHCP server log for the Ethernet Base MAC address shown on the AP label and take note of the corresponding IP address.

- 4 Relaunch the AP management tool, this time using: **https://<IP address discovered in previous step>**, to continue configuring the AP. See the Caution regarding “**WIRELESS SECURITY**” on page 53.

To access additional network resources



- 1 To access network resources other than just the Internet, select **VSC > Profiles** and select the appropriate profile. The default is *Alvarion Ltd..*
- 2 In the **Add/Edit Virtual Service Community page**, clear the **Wireless security filters** checkbox and select **Save**.

To connect to an Alvarion access controller



- 1 Select **VSC > Profiles** and select the appropriate profile.
- 2 Under **General**, select the **Use Alvarion access controller** checkbox, and select **Save**.

To assign an IP address



If your Internet service provider or network administrator requires a different configuration, for example a static IP address assignment:

- 1 From the AP management tool, select **Network > Ports > Bridge port** and choose another option in the **Assign IP address via** box.

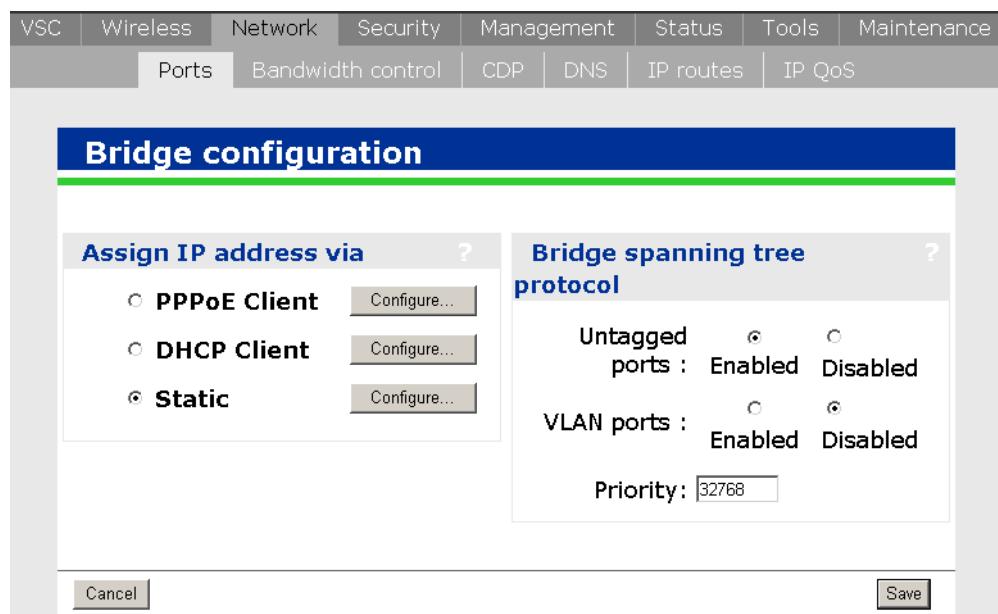
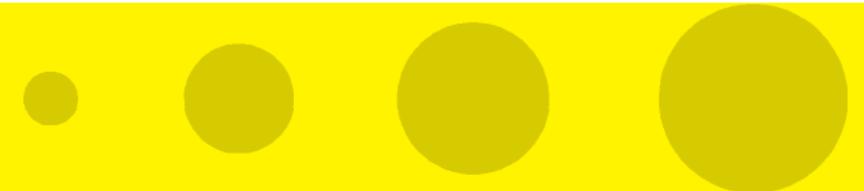


Figure 4-6: Bridge Configuration Window

- 2 Select the corresponding **Configure** button and configure as instructed. For more information see “[Port Configuration](#)” on page 110.



5

Chapter 5 - Working with Virtual Networks

In This Chapter:

- “Key Concepts” on page 62
- “Virtual Network Configuration Overview” on page 69
- “Virtual Network Configuration Options” on page 72
- “Virtual Network Data Flow” on page 80
- “Quality of Service (QoS)” on page 84

5.1 Key Concepts

A VSC (virtual network) is a collection of configuration settings that define key operating characteristics of an AP. In most cases, a virtual network is used to define the characteristics of a wireless network.



TIP

The Deployment Guide provides numerous detailed examples on virtual network configuration when using the service controller with both controlled and autonomous APs.

Multiple virtual network definitions can be created to enable support for different types of users. For example, in the following scenario, four virtual networks are used. Each virtual network is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to set the priority of user traffic.

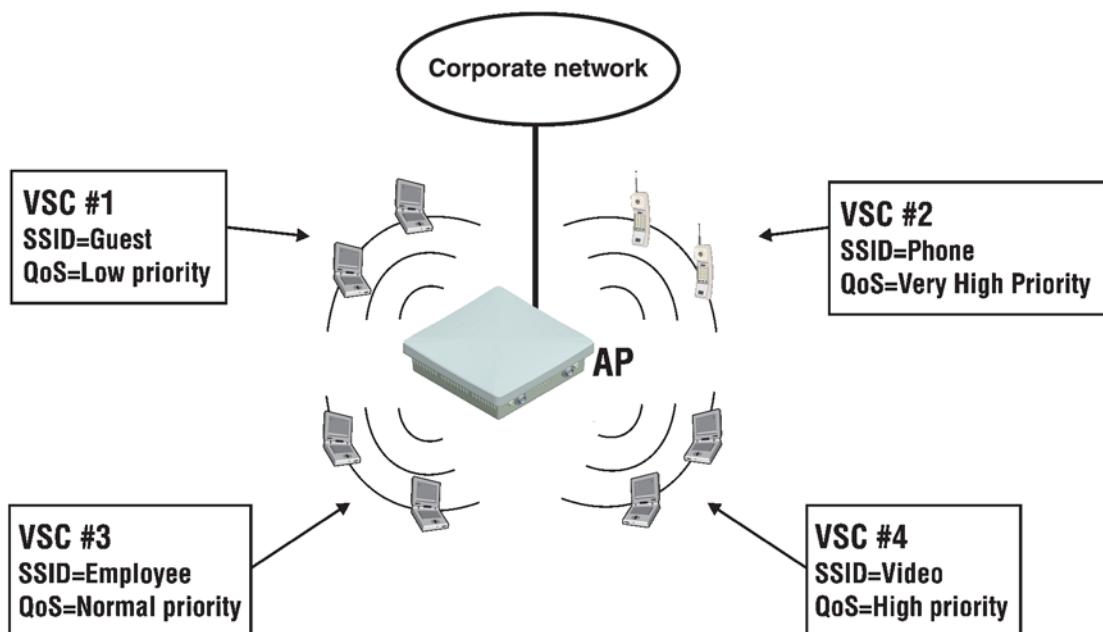


Figure 5-1: Four Virtual Networks

5.1.1 Stand-alone Deployment

An autonomous MAP can be deployed as a stand-alone device to provide wireless networking support for an existing wired network. The AP essentially creates a wireless extension to the existing wired network, bridging wireless users onto the wired backbone.

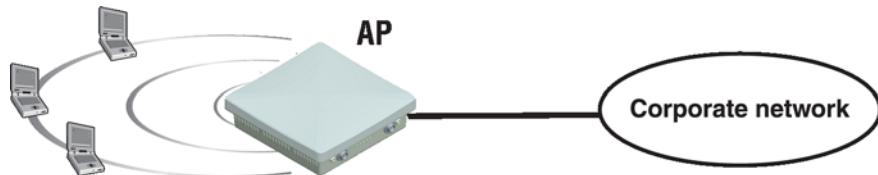


Figure 5-2: Stand-alone Deployment

5.1.1.1 User Authentication

The AP can validate user login credentials using a third-party RADIUS server. The following authentication types are supported: WPA / WPA2, 802.1X, and MAC.

5.1.1.1.1 WPA / WPA2 and 802.1X Authentication

Full support is provided for users with 802.1X or WPA / WPA2 client software, and 802.1X client software that uses the following:

- EAP-TLS: Extensible Authentication Protocol Transport Layer Security.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security.
- PEAP: Protected Extensible Authentication Protocol.

NOTE



For security reasons, use of 802.1X without enabling dynamic WEP encryption is not recommended.

5.1.1.1.2 MAC-based Authentication

Devices can be authenticated based on their MAC address. This is useful for authenticating devices that do not have a web browser (cash registers, for example). As soon as the device's MAC address appears on the network, the MAP attempts to authenticate them.

5.1.1.2 Using More Than One Authentication Type in a Virtual Network

For added flexibility, you can enable both the 802.1X and Virtual Networks-based MAC authentication at the same time. The following table shows the results for all authentication scenarios.

NOTE

MAC authentication always takes place first. If it fails, 802.1X is then attempted.

Active Authentication Method	Authentication result		Network Access?
	MAC	802.1X	
MAC	Failure	-	No
	Success	-	Yes
802.1X optional	-	Success	Yes
	-	Failure	No
	-	-	Yes
802.1X mandatory	-	Failure	No
	-	Success	Yes
	-	-	No
MAC optional + 802.1X optional	Failure	-	No
		Success	Yes
		Failure	No
	Success	Failure	No
		-	Yes
		Success	Yes
MAC optional + 802.1X mandatory	Failure	-	No
		Success	Yes
		Failure	No
	Success	Failure	No
		-	No
		Success	Yes
MAC mandatory+ 802.1X optional	Failure	-	No
		Success	No
		Failure	No
	Success	Failure	No
		-	Yes
		Success	Yes

Active Authentication Method	Authentication result		Network Access?
	MAC	802.1X	
MAC mandatory+ 802.1X mandatory	Failure	-	No
		Success	No
		Failure	No

5.1.1.2.1 Authentication Examples

5.1.1.2.1.1 MAC and 802.1X enabled, mandatory 802.1X authentication disabled

Wireless client stations are automatically authenticated by their MAC address.

- **If MAC authentication succeeds,** the client station gains access. Next, the client station can initiate an 802.1X session, causing 802.1X authentication to take place. The result of this authentication then takes precedence over the MAC authentication result.
- **(When MAC mandatory disabled.) If MAC authentication fails,** the client station does not gain access but can still initiate an 802.1X session, causing 802.1X authentication to take place. If the result of this authentication is successful, then the client station gains access.
- **(When MAC mandatory enabled.) If MAC authentication fails,** the client station does not gain access regardless of the 802.1X result.

5.1.1.2.1.2 MAC and 802.1X Enabled, Mandatory 802.1X Authentication Enabled

Wireless client stations are automatically authenticated by their MAC address. If MAC authentication succeeds they do not gain access until 802.1X authentication is successful.

5.1.1.2.1.3 MAC Disabled and 802.1X Enabled, Mandatory 802.1X Authentication Disabled

Wireless client stations automatically gain access to the network with no authentication required. If the client station starts an 802.1X session, authentication takes place. If the result of this authentication is failure, then the client station loses access to the network.

5.1.1.2.1.4 MAC Disabled and 802.1X Enabled, Mandatory 802.1X Authentication Enabled

Wireless client stations gain access to the network only after successful 802.1X authentication.

5.1.2 Deployment in Conjunction with an Alvarion Service Controller

Autonomous APs can also be used in conjunction with a service controller to create a public access network infrastructure. In this type of deployment, all virtual network are access-controlled, which means that the AP forwards all wireless user traffic to the service controller which handles user authentication and access control.

To reach protected network resources, wireless users must successfully authenticate with the public access interface that is provided by the service controller.

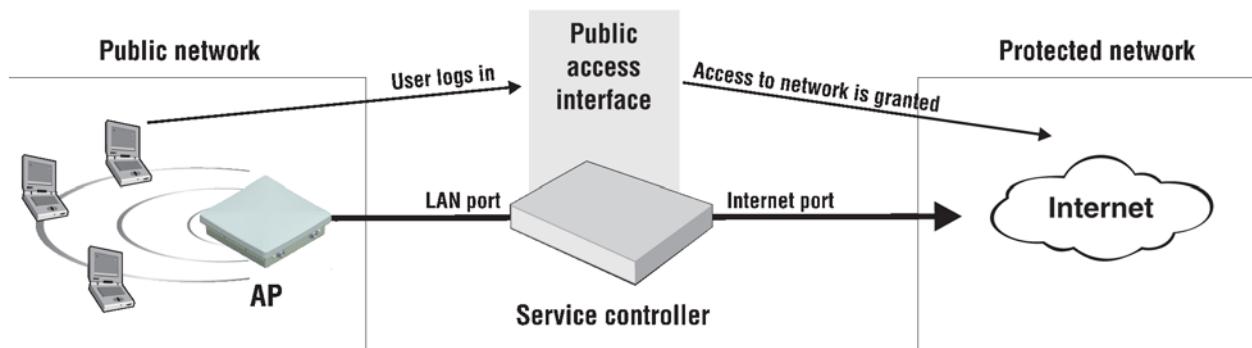


Figure 5-3: Deployment in Conjunction with an Alvarion Service Controller

The following authentication types are supported on the service controller: WPA / WPA2, 802.1X, MAC, HTML. For more information on service controller authentication features, see the service controller's *Admin Guide*.

In this type of installation, virtual network definitions on both the AP and service controller must match so that traffic from wireless users connected to the AP can be sent to the service controller for handling. For example, if two virtual networks are being used, they could be configured as follows:

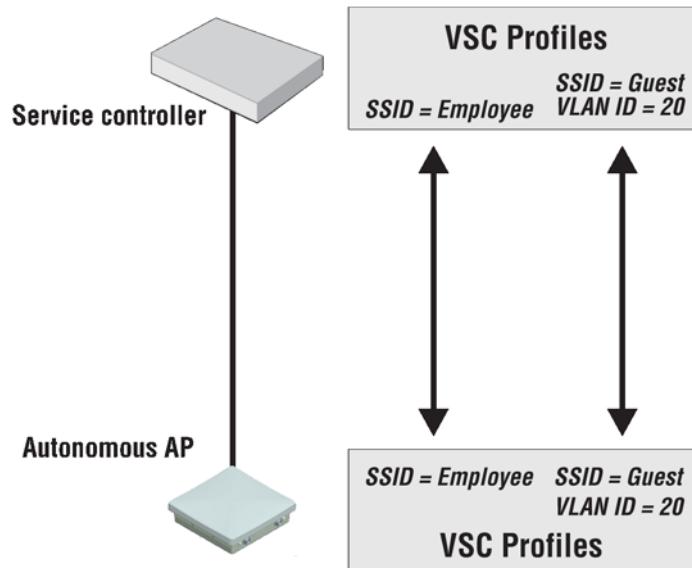


Figure 5-4: Example of Configuration of Two Virtual Networks

5.1.3 Management with VLANs

When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the Virtual Networks on both the autonomous AP and the service controller as illustrated.

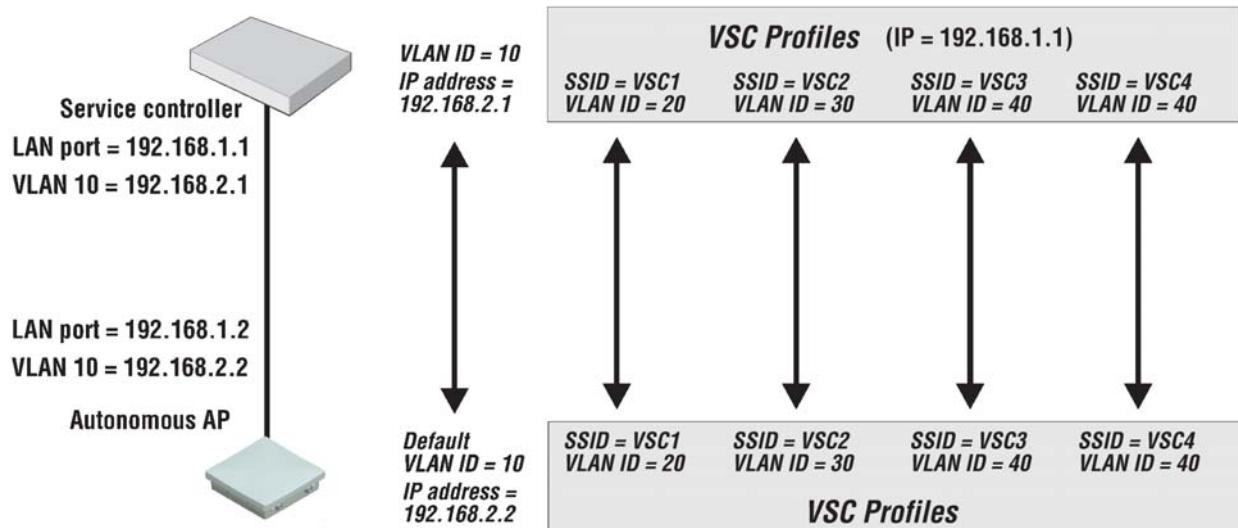


Figure 5-5: Management with VLANs

In this example, the traffic for each wireless network is carried on its own VLAN. This leaves only management traffic from the autonomous AP on VLAN 10. A static IP is assigned on both ends to permit the two devices to communicate.

5.2 Virtual Network Configuration Overview

The VSC page lists the VSC defined virtual network profiles.

The screenshot shows the 'Virtual Service Communities' page with a single profile listed:

Name	Ingress SSID	Egress VLAN	QoS	Filtering IP MAC	Encryption TKIP AES WEP	Authentication 802.1x	MAC
Alvarion Networks	Alvarion Network	-	DiffSrv	- -	- - -	-	-

Below the table are two buttons: 'Add New VSC Profile...' and a legend:

- Key = Use access controller
- Off = SSID
- On = SSID
- On and configured for broadcast

Figure 5-6: VSC Page

To edit a profile, select its link in the **Name** column. To add a new profile, select **Add New VSC Profile**. The **Add/Edit Virtual Service Community** page opens providing all virtual network profile options.

The screenshot shows the 'Add/Edit Virtual Service Community' page with the following configuration:

- General** tab:
 - Name: Corporate
 - Use access controller
- Virtual AP** tab:
 - Virtual AP
 - WLAN** section:
 - Name (SSID): Corporate
- Wireless protection** tab:
 - Wireless protection: WPA
 - Mode: WPA2 (AES/CCMP)
 - Key source: RADIUS
 - RADIUS profile: Access controller
 - Station ID delimiter: Dash: '-'
 - Station ID MAC case: Upper case

Figure 5-7: Adding a New Profile

5.2.1 About the ‘Use Alvarion Access Controller’ Option

Availability of certain virtual network features and their functionality are dependent on the setting of the **Use Alvarion access controller** in the virtual network’s **General** box. This option determines how authentication and access control are handled by the virtual network:



Figure 5-8: ‘Use Alvarion Access Controller’ Option

5.2.1.1 If “Use Alvarion Access Controller” is Enabled

This creates an access-controlled virtual network. This means that the AP must be used in conjunction with an Alvarion access controller, because the virtual network is automatically configured to forward all user traffic to the access controller for authentication (**Wireless protection** and **MAC-based authentication** options are forced to use an Alvarion access controller as the RADIUS server). Also, once authenticated, user traffic is restricted by the **Wireless security filters** option. Only traffic addressed to the access controller is permitted. (These filters can be disabled if required.)

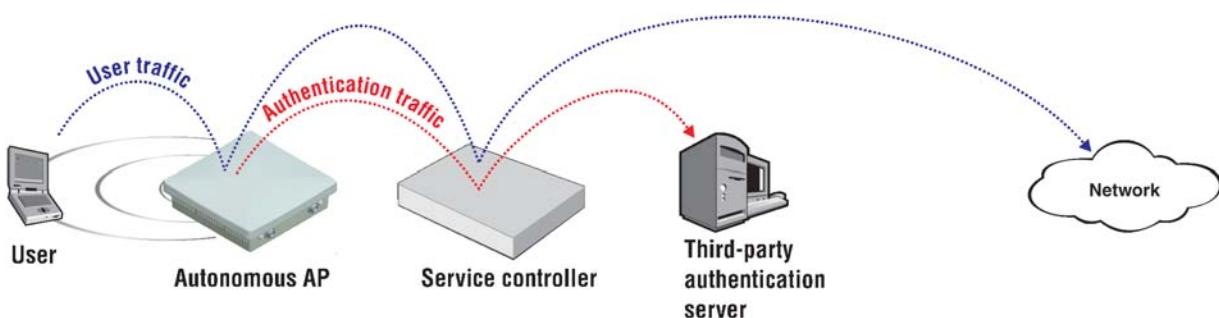


Figure 5-9: An Access-controlled Virtual Network

5.2.1.2 If “Use Alvarion Access Controller” is Disabled

This creates a non access-controlled virtual network, which allows the AP to manage user authentication using the services of a third-party RADIUS server. Once authenticated, user traffic is restricted to the default gateway assigned to

the AP by the **Wireless security filters** option. (These filters can be disabled or re-configured if required.).

NOTE

When access control is disabled, user traffic sent by the AP must bypasses the service controller, otherwise it will be interpreted and processed.

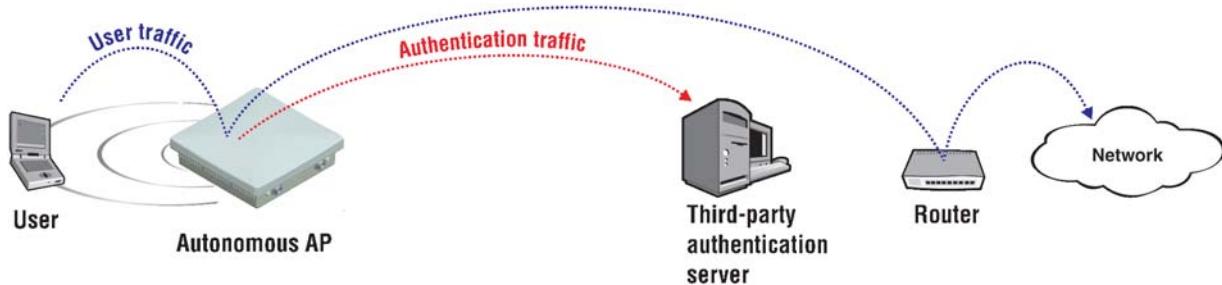


Figure 5-10: ‘Use Alvarion Access Controller’ Option is Disabled

5.3 Virtual Network Configuration Options

The following table lists the Virtual Network configuration options that are available depending on how the **Use Alvarion access controller** option is configured.

Virtual Network configuration option	Use Alvarion access controller is:	
	Enabled	Disabled
Virtual AP	X	X
Egress VLAN	X	X
Wireless security filters	User traffic restricted to access controller	User traffic restricted to default gateway. Can be changed.
Wireless protection	User authentication is performed by the access controller.	User authentication is performed by any external RADIUS server
MAC-based authentication	User authentication is performed by the access controller.	User authentication is performed by any external RADIUS server
Location-aware	X	
Wireless MAC filter	X	X
Wireless IP filter	X	X

This sections that follow provide an overview of each virtual network option and how it can be used. For complete descriptions of individual parameters refer to the online help in the management tool.

5.3.1 Virtual AP

These settings define the characteristics of the wireless network created by the virtual network, including its name, the number of clients supported, and quality of service settings (see “[Quality of Service \(QoS\)](#)” on page 84).

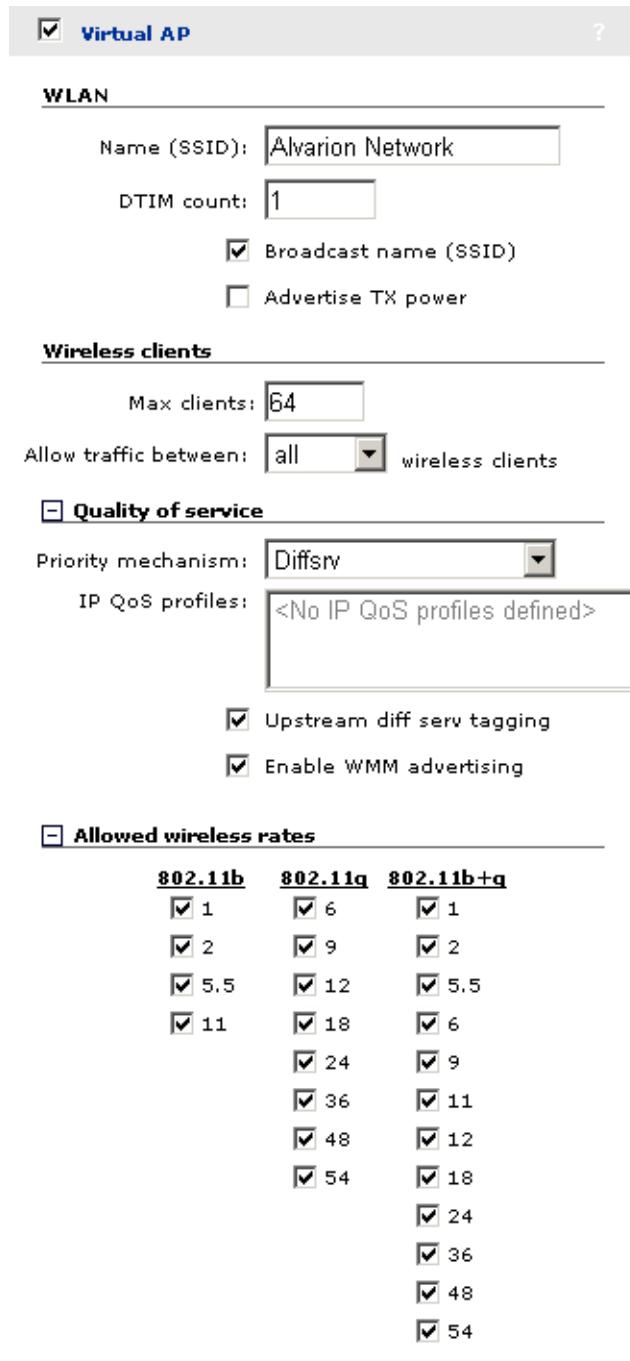


Figure 5-11: Virtual AP

5.3.2 Egress VLAN

Sets the VLAN that this profile forwards data traffic to. If you do not select a VLAN, traffic is sent untagged. Note however, that a VLAN may still be assigned on

a per-customer basis via a setting in the customer's RADIUS account (if using RADIUS-based authentication). Also, a global VLAN setting is available on the **Network > Ports** page which will tag all traffic sent on port 1 and 2.

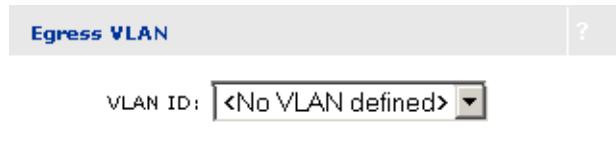


Figure 5-12: Egress VLAN

In the above example, with all defaults selected, the MAP bridges all wireless traffic to the wired LAN.

5.3.3 Wireless Security Filters

APs feature an intelligent bridge that can apply security filters to safeguard the flow of wireless traffic. These filters limit both incoming and outgoing traffic as defined below and force the APs to exchange traffic with a specific upstream device.

- If **Use Alvarion access controller** is enabled (under **General**), the AP will only forward user traffic that is addressed to the service controller. All other traffic is blocked. Make sure that the service controller is set as the default gateway. If not, all user traffic will be blocked by the AP.

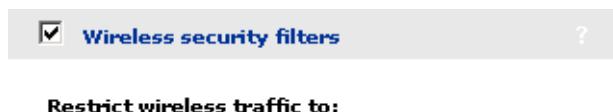


Figure 5-13: Wireless Security Filters

- If **Use Alvarion access controller** is disabled (under **General**), then the security filters can be used to block traffic unless it is addressed to a specific device.



Figure 5-14: Security Filters When ‘Use Alvarion Access Controller’ is disabled

Use the **Custom** option to define a custom filter with standard pcap syntax and a few Alvarion-specific placeholders. See the online help for details.

5.3.4 Wireless Protection

Three types of wireless protection are offered. WPA, 802.1X, and WEP.

5.3.4.1 WPA

This option enables support for users with WPA / WPA2 client software. Support is provided for

- **WPA (TKIP)**: WPA with TKIP encryption.
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with CCMP encryption.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time.

Authentication must occur via an external device (unless preshared keys are used). If **Use Alvarion access controller** is enabled (under **General**), this must be an Alvarion access controller, otherwise a third-party RADIUS server can be used.

Use Alvarion access controller	
Enabled	Disabled
<input type="checkbox"/> Wireless protection WPA Mode: WPA (TKIP) Key source: RADIUS RADIUS profile: [Access controller] Station ID delimiter: Dash: '-' Station ID MAC case: Uppercase	<input type="checkbox"/> Wireless protection WPA Mode: WPA (TKIP) Key source: RADIUS RADIUS profile: <No RADIUS defined> <input type="checkbox"/> RADIUS accounting RADIUS profile: <No RADIUS defined> Called-Station-Id Content: BSSID Station ID delimiter: Dash: '-' Station ID MAC case: Uppercase

5.3.4.2 802.1X

This option enables support for users with 802.1X client software that use any of the following authentication methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.

Additionally, when an external RADIUS server is used, support for EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC is also provided. Check your external RADIUS server for supported authentication methods.

Authentication must occur via an external device. If **Use Alvarion access controller** is enabled (under **General**), this must be an Alvarion access controller, otherwise a third-party RADIUS server can be used.

Use Alvarion access controller	
Enabled	Disabled
<input type="checkbox"/> Wireless protection [802.1X] ? RADIUS profile: [Access controller] <input type="checkbox"/> WEP encryption <input checked="" type="checkbox"/> Mandatory authentication Station ID delimiter: Dash: <input type="text" value="4"/> Station ID MAC case: Upper case	<input type="checkbox"/> Wireless protection [802.1X] ? RADIUS profile: <No RADIUS defined> <input type="checkbox"/> RADIUS accounting RADIUS profile: <No RADIUS defined> <input type="checkbox"/> WEP encryption <input checked="" type="checkbox"/> Mandatory authentication Called-Station-Id Content: BSSID Station ID delimiter: Dash: <input type="text" value="4"/> Station ID MAC case: Upper case

NOTE

For security reasons, using 802.1X without enabling at least WEP encryption is not recommended.

When the **Mandatory** option is enabled, all wireless users must authenticate using 802.1X, regardless of whether other methods are active. For more information, see “[Using More Than One Authentication Type in a Virtual Network](#)” on page 63

5.3.4.3 WEP

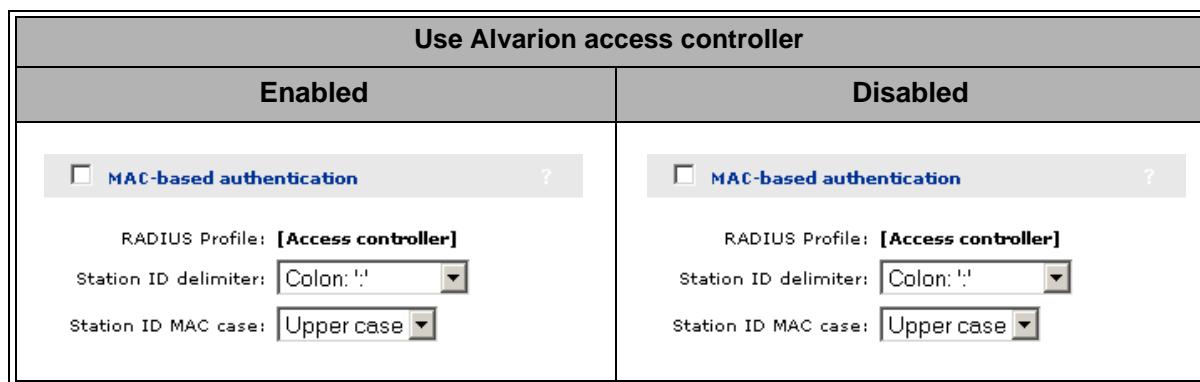
This option provides support for users using WEP encryption.

<input type="checkbox"/> Wireless protection [WEP] ?
Key: <input type="text"/>
Key format: <input checked="" type="radio"/> ASCII <input type="radio"/> HEX

Figure 5-15: WEP

5.3.5 MAC-based Authentication

This option enables wireless users to be authenticated by their MAC addresses. Authentication must occur via an external device. If **Use Alvarion access controller** is enabled (under **General**), this must be an Alvarion access controller, otherwise a third-party RADIUS server can be used.



5.3.6 Location-aware

This feature enables you to control logins to the public access network based on the AP, or group of APs, to which a user is connected. It is only available when **Use Alvarion access controller** is enabled (under **General**).

For each user login, location-aware sends the PHY Type, SSID, and VLAN to the access controller. It also includes the specified **Group name**.



Figure 5-16: Location-aware

5.3.7 Wireless MAC Filter

This option allows or you to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses. You can either block or allow access.

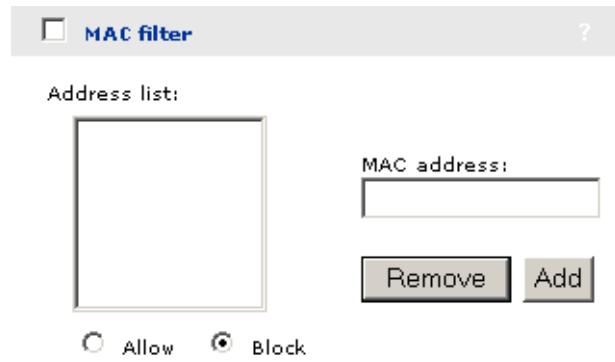


Figure 5-17: Wireless MAC Filter

5.3.8 Wireless IP Filter

This option enables you to only allow wireless-to-wired LAN traffic for specific destination addresses.

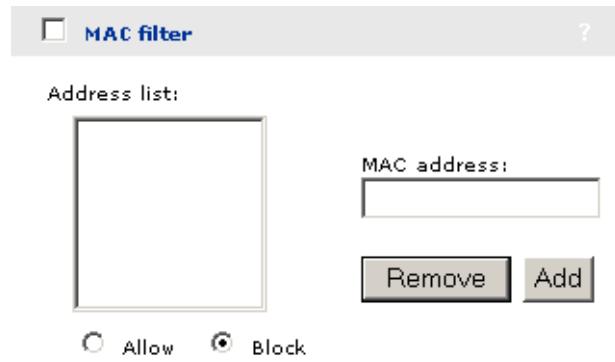


Figure 5-18: Wireless IP Filter

NOTE

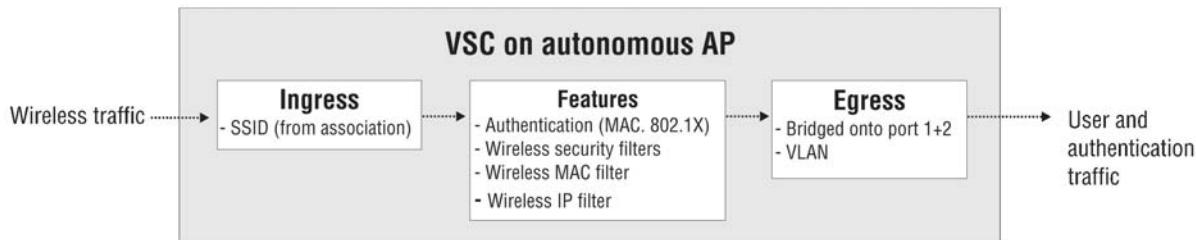


This option is applies on a per-radio basis.

5.4 Virtual Network Data Flow

Each Virtual Network provides a number of configurable options. The following diagrams illustrate how traffic from wireless users is handled by virtual network definitions on an AP and service controller, and shows the options that apply on each device.

Stand-alone deployment



AP deployed with a service controller

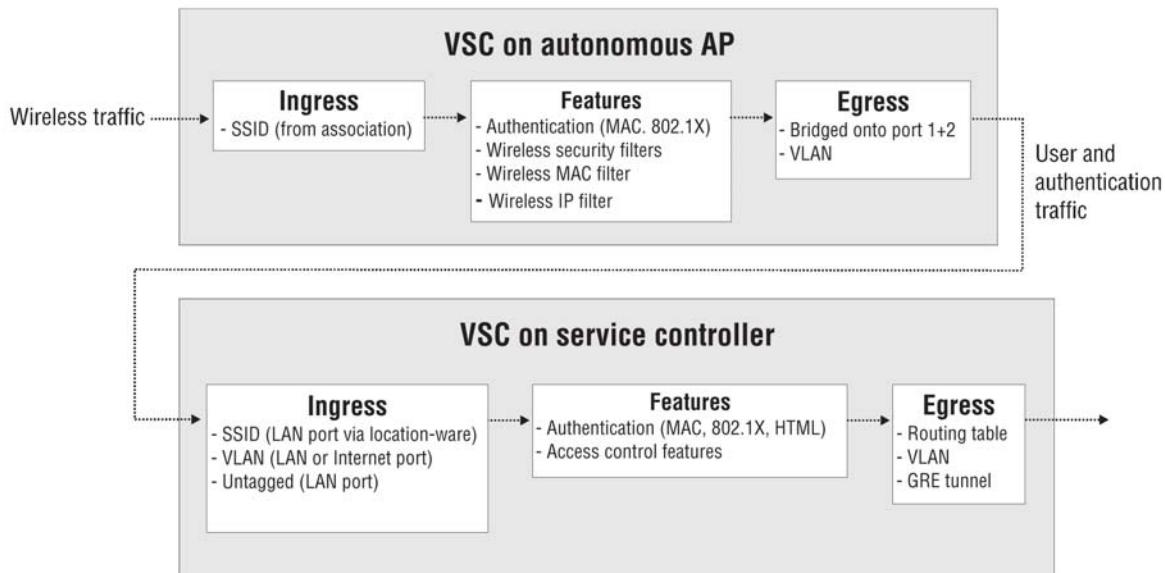


Figure 5-19: Virtual Network Data Flow

5.4.1 Stand-alone Deployment

5.4.1.1 Virtual Network on Autonomous AP

5.4.1.1.1 Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

5.4.1.1.2 Features

- **Authentication:** Authentication can be either 802.1X or MAC. To validate user credentials the AP makes use of an external RADIUS server, which can be the service controller or a third-party device. For more information, see “Authenticating Administrators Using a RADIUS Server” on page 129.
- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific device (like the service controller). For more information, see “Wireless Security Filters” on page 74.
- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

5.4.1.1.3 Egress

- **Bridge onto port 1+2:** Unless a centralized mode tunnel has been established, user and authentication traffic is bridged onto ports 1 and 2.
- **VLAN:** All traffic on port 1 or 2 can be assigned to a VLAN.

5.4.2 AP deployed with an Alvarion Service Controller

5.4.2.1 Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

5.4.2.2 Features

- **Authentication:** Authentication can either 802.1X or MAC. To validate user credentials the AP makes use of the service controller. For more information, see “Authenticating Administrators Using a RADIUS Server” on page 129.
- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific device (like the service controller). For more information, see “Wireless Security Filters” on page 74.
- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

5.4.2.3 Egress

- **Bridge onto port 1+2:** User and authentication traffic is bridged onto ports 1 and 2.
- **VLAN:** All traffic on port 1 or 2 can be assigned to a VLAN.

5.4.3 Virtual Network on Service Controller

For more information on service controller feature configuration, refer to the service controller’s *Admin Guide*.

5.4.3.1 Ingress

- **SSID (LAN port):** SSID is retrieved using the location-ware function client runs on AP.
- **VLAN (LAN or Internet port):** Traffic with a VLAN ID is handled by the Virtual Network with a matching VLAN definition.
- **Untagged (LAN port):** Untagged traffic on the LAN port may originate from wired users, or APs operating in autonomous mode (Alvarion or third-party).

5.4.3.2 Features

- **Authentication:** The service controller supports 802.1X, MAC, or HTML authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS).
- **Access control features:** The service controller provides a number of features that can be applied to user sessions. Features can be enabled globally or on a per-account basis. For more information.

5.4.3.3 Egress

The service controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or IP GRE tunnel.

5.5 Quality of Service (QoS)

The MAP features a quality of service (QoS) implementation that provides a wide range of methods for traffic prioritization.

5.5.1 QoS Priority Mechanism

The QoS priority mechanism defines four traffic queues based on the WMM standard. In order of priority, these queues are:

Queue	Typically used for
1	Voice traffic
2	Video traffic
3	Best effort data traffic
4	Background data traffic

Each QoS priority option maps traffic to one of the four traffic queues. Users that do not support the QoS priority option defined on a virtual network are always assigned to queue 3.

QoS priority is only applied to wireless traffic sent by APs to wireless users with the following exception: If a virtual network-based priority setting is selected and egress traffic is assigned to a VLAN then the Virtual Network-based priority settings are mapped to a corresponding 802.1p value for all incoming traffic received from wireless clients and forwarded onto the VLAN. For example, if Virtual Network-based priority **High** is selected, then traffic from wireless clients will be mapped to the appropriate 802.1p value for queue 2.

NOTE



Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

5.5.1.1 SVP Support

Spectralink Voice Protocol is an open standard for the prioritization of voice traffic on wireless and wired LANs. SVP traffic is sent on queue 1 for all priority mechanisms except Virtual Network-based.

5.5.1.2 802.1p

802.1p traffic is classified based on the VLAN priority field present within the VLAN header.

Queue	Traffic type (based on VLAN priority field)
1	SVP traffic
1	6,7
2	4,5
3	0,2
3	Other traffic
4	1,3

NOTE



To support 802.1p, the Virtual Network must have an egress VLAN assigned to it.

5.5.1.3 Virtual Network-based Priority

The virtual network-based priority mechanism is unique to Alvarion Ltd. APs. It enables you to specify a priority level for all traffic on a virtual network. This enables users that do not have a QoS mechanism to set traffic priority by connecting to the appropriate SSID.

If you enable a virtual network-based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated users. For example, if you set **VSC-Based Low Priority** for a Virtual Network, all devices that connect to the virtual network have their traffic set at this priority

Queue	Description
1	Very High
2	High
3	Normal
4	Low

NOTE



Reserve **Virtual Network-Based Very-high** priority for voice and other critical applications.

5.5.1.4 Differential Services (DiffServ)

Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which maps to the appropriate traffic queue.

Queue	Traffic type (based on binary value of Class Selector Codepoint)
1	SVP traffic
1	111000 (Network control)
1	110000 (Internetwork control)
2	101000 (Critical)
2	100000 (Flash override)
3	011000 (Flash)
3	000100 (Routine)
4	010000 (Immediate)
4	001000 (Priority)
3	Other traffic

5.5.1.5 TOS

The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.

Queue	Traffic type
1	SVP traffic
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
3	Non-TOS traffic
4	All other TOS traffic

5.5.1.6 IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. For more information, see “IP QoS” on page 122.

5.5.1.7 Disabled

When QoS traffic prioritization is disabled, all traffic on the virtual network is sent to queue 3.

5.5.1.8 QoS Example

In this QoS example a single MAP provides voice and data wireless support with different quality of service settings for guests and employees.

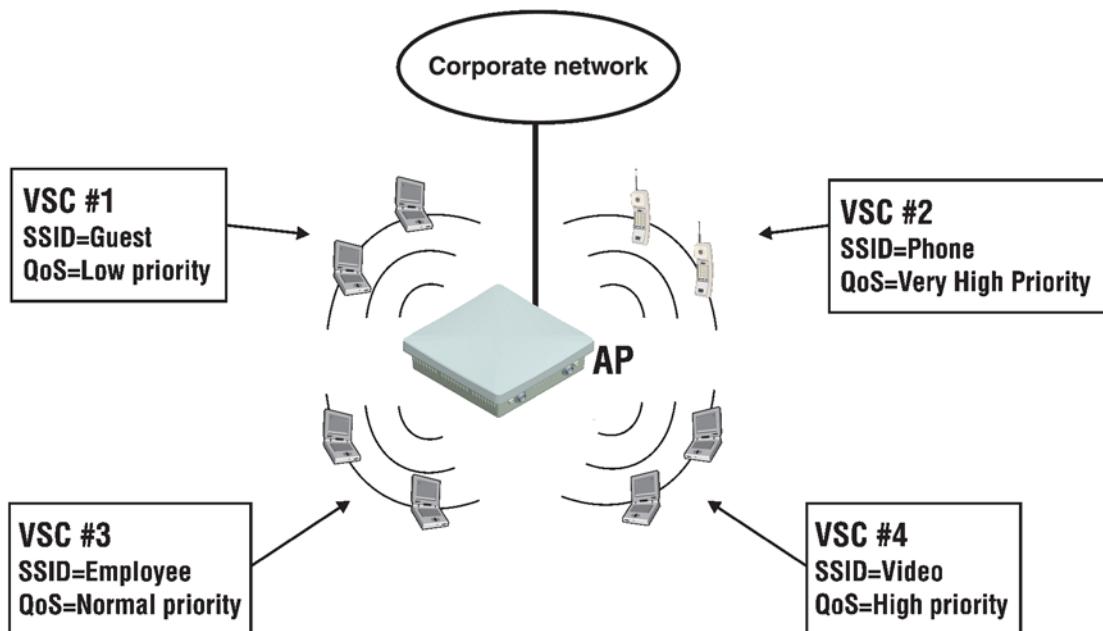


Figure 5-20: QoS Example

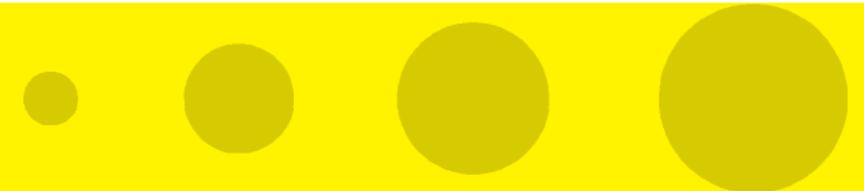
virtual networks define the following SSIDs:

- **Voice:** Supports wireless phones using the the Very High Priority mechanism.
- **Video Conference:** Supports high-priority video traffic for video conferences.
- **Data:** Used by employees. Features a higher QoS setting than the guest profile.
- **Guest:** Used by guests. Guest get the lowest traffic priority, to reserve bandwidth for employees.



TIP

For more examples of QoS implementation, see the Deployment Guide.



6

Chapter 6 - Wireless Configuration

In This Chapter:

- “Wireless Coverage” on page 90
- “Conducting a Site Survey” on page 97
- “Radio Configuration” on page 100

6.1 Wireless Coverage

As a starting point for planning your network, you can assume that when operating at high power, the AP's radio provides a wireless networking area (also called a wireless cell) of up to 300 feet (100 meters) in diameter. Before creating a permanent installation however, you should always perform a site survey to determine the optimal settings and location for the AP.

The following sections provide information on wireless coverage. A tool that can help simplify planning a secure wireless network is the Alvarion RF Planner. For more information, see the *RF Planner Admin Guide*.

NOTE



Supported wireless modes, operating channels, and power output are determined by the regulations of the country in which the AP is operating, and are controlled by the country setting on the AP. For more information, see “[Country](#)” on page 141.

6.1.1 Wireless Mode

Supported wireless modes may include the following:

- 802.11b: Up to 11 Mbps in the 2.4 GHz frequency band.
- 802.11g: Up to 54 Mbps in the 2.4 GHz frequency band.
- 802.11 b + g: Up to 11 Mbps and 54 Mbps in the 2.4 GHz frequency band.

6.1.2 Factors Limiting Wireless Coverage

Wireless coverage is affected by the factors discussed in this section.

6.1.2.1 Radio Power

More radio power means better signal quality and the ability to create bigger wireless cells. However, cell size should generally not exceed the range of transmission supported by wireless users. If it does, users will be able to receive signals from the AP but will not be able to reply, rendering the connection useless.

Further, when more than one AP operates in an area, you must adjust wireless cell size to reduce interference between APs. An automatic power control feature is available to address this challenge. For details, see “[Transmit Power Control](#)” on page 104.

6.1.2.2 Antenna Configuration

Antennas play a large role in determining the shape of the wireless cell and transmission distance. Consult the specifications for the antennas you use to determine how they affect wireless coverage.

6.1.2.3 Interference

Interference is caused by other APs or devices that operate in the same frequency band as the AP and can substantially affect throughput. Advanced wireless configuration features are available to automatically eliminate this problem. For details, see “[Radio Configuration](#)” on page 100.

In addition, the several tools are available to diagnose interference problems as they occur.

- Select **Wireless > Neighborhood** to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies. This wireless neighborhood feature also makes it easy for you to find rogue APs. For more information see “[Conducting a Site Survey](#)” on page 97.
- Select **Status > Wireless** to view detailed information about packets sent and received, transmission errors, and other low-level events.
- Select **Status > Client data rate matrix** to view information about data rates for all connected client stations. This makes it easy to determine if low-speed clients are affecting network performance. To prevent low-speed clients from connecting, you can use the **Allowed wireless rates** option when defining a Virtual Network. For more information, see “[Virtual AP](#)” on page 72.

IMPORTANT



APs that operate in the 2.4 GHz band may experience interference from 2.4 GHz cordless phones and microwave ovens.

6.1.2.4 Physical Characteristics of the Location

To maximize coverage of a wireless cell, wireless APs are best installed in an open area with as few obstructions as possible. Try to choose a location that is central to the area being served.

Radio waves cannot penetrate metal; they are reflected instead. A wireless AP can transmit through wood or plaster walls and closed windows; however, the steel reinforcing found in concrete walls and floors may block transmissions or reduce

signal quality by creating reflections. This can make it difficult or impossible for a single AP to serve users on different floors in a concrete building. Such installations require a separate wireless AP on each floor.

6.1.3 Configuring Overlapping Wireless Cells

Overlapping wireless cells occur when two or more APs are within transmission range of each other. This may be under your control, (for example, when you use several cells to cover a large location), or out of your control (for example, when your neighbors set up their own wireless networks). In either case, the problems you face are similar.

6.1.3.1 Performance Degradation and Channel Separation

When two wireless cells operating on the same frequency overlap, throughput can be reduced in both cells. Reduced throughput occurs because a wireless user that is attempting to transmit data defers (delays) transmission if another station is transmitting. In a network with many users and much traffic, these delayed transmissions can severely affect performance, because wireless users may defer several times before the channel becomes available. If a wireless user is forced to delay transmission too many times, data can be lost.

Delays and lost transmissions can severely reduce throughput on a network. To view this information about your network, select **Status > Wireless**. For recommendations on using this information to diagnose wireless problems, see the online help for this page.

The following example shows two overlapping wireless cells operating on the same frequency. Since both APs are within range of each other, the number of deferred transmissions can be large.

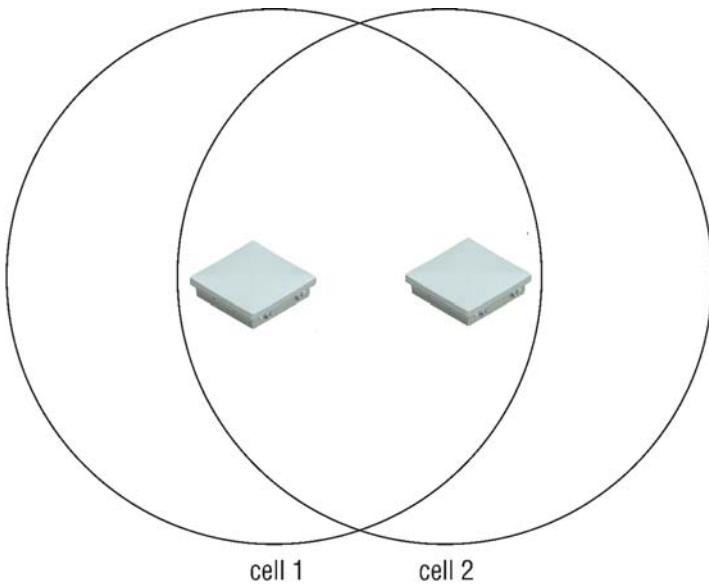


Figure 6-1: Overlapping Wireless Cells Operating on the Same Frequency

The solution to this problem is to set the two networks to different channels with as great a separation as possible in their operating frequencies. This reduces crosstalk and enables client stations connected to each AP to transmit at the same time.

6.1.3.2 Selecting Channels

For optimal performance when operating in 802.11b or 802.11g modes, select an operating frequency that is different by at least 25 MHz from the frequency used by other wireless APs that operate in neighboring cells.

Two channels with the minimum 25 MHz frequency separation always perform *worse* than two channels that use maximum separation. It is always best to use the greatest separation possible between overlapping networks.

With the proliferation of wireless networks, it is very possible that the wireless cells of APs outside your control overlap your intended area of coverage. To choose the best operating frequency, select **Wireless > Neighborhood** to generate a list of all APs that operate near you and their operating frequencies.

The set of available channels is automatically determined based on the **Country** setting you define by selecting **Management > Country**. This means that the number of non-overlapping channels available to you varies by geographical location, which affects how you set up your multi-cell network.

6.1.3.2.1 Sample Channel Selections

For example, when operating in 802.11b mode, the AP supports the following 14 channels in the 2.4 GHz band.

Channel	Frequency
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2477

However, the number of channels available for use in a particular country are determined by the regulations defined by the local governing body. The following table shows the number of channels that are available in North America, Japan, and Europe.

Region	Available channels
North America	1 to 11
Japan	1 to 14
Europe	1 to 13

Since the minimum recommended separation between overlapping channels is 25 MHz (five cells) the recommended maximum number of overlapping cells you can have in most regions is three. The following table gives examples relevant to North America, Japan, and Europe.

North America	Japan	Europe
■ cell 1 on channel 1	■ cell 1 on channel 1	■ cell 1 on channel 1
■ cell 2 on channel 6	■ cell 2 on channel 7	■ cell 2 on channel 7
■ cell 3 on channel 11	■ cell 3 on channel 14	■ cell 3 on channel 13

In North America you can create an installation as shown in the following figure.

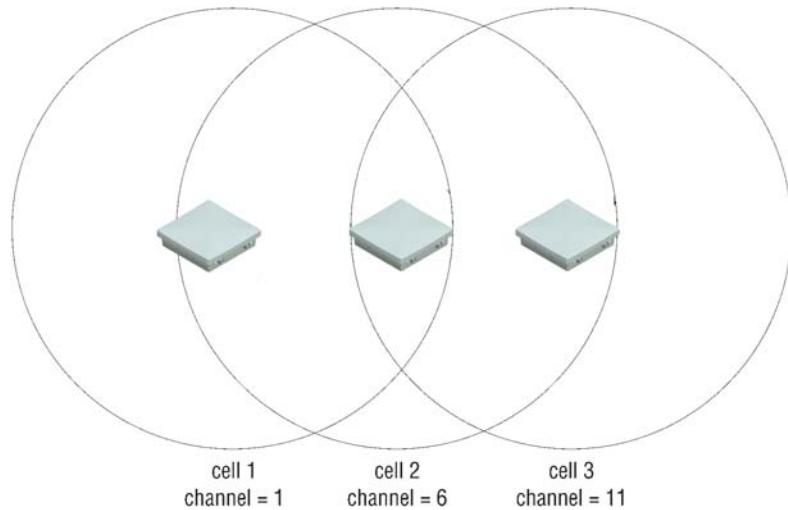


Figure 6-2: Example of Three Overlapping Cells

Reducing transmission delays by using different operating frequencies in North America.

Alternatively, you can stagger cells to reduce overlap and increase channel separation, as shown in the following figure.

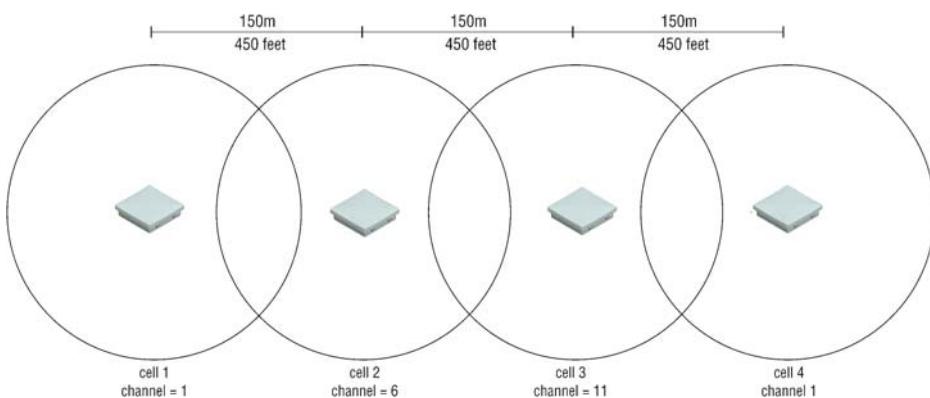


Figure 6-3: Reducing Overlap to Increase Channel Separation

Using only three frequencies across multiple cells in North America.

This strategy can be expanded to cover an even larger area using three channels, as shown in the following figure.

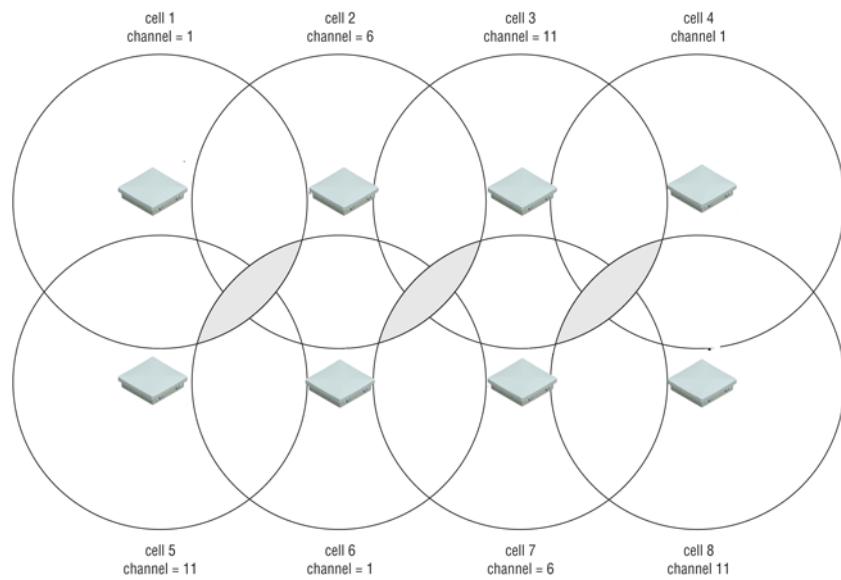


Figure 6-4: Using Three Frequencies Across Multiple Cells

Using three frequencies to cover a large area in North America. Gray areas indicate overlap between two cells that use the same frequency.

6.1.3.2.2 Distance Between APs

In environments where the number of wireless frequencies is limited, it can be beneficial to adjust the receiver sensitivity of the AP. To make the adjustment, select **Wireless > Radio(s)** and set the **Distance between access points** option.

For most installations, **Distance between access points** should be set to **Large**. However, if you are installing several wireless APs and the channels available to you do not provide enough separation, reducing receiver sensitivity can help you to reduce the amount of crosstalk between wireless APs.

Another benefit to using reduced settings is that it improves roaming performance. Wireless users switch between APs more frequently.

6.1.3.3 Automatic Power Control

The automatic power control feature enables the AP to dynamically adjust its transmission power to avoid causing interference with neighboring Alvarion APs. For information see “[Transmit Power Control](#)” on page 104.

6.2 Conducting a Site Survey

You can use the wireless neighborhood feature to conduct a site survey to discover the operating frequencies of other APs in your area.

Select **Wireless > Neighborhood** and then select **Repeat scan every** and set the desired interval. The AP scans at the specified interval to find all active APs. For example:

The screenshot shows the 'Wireless neighborhood' configuration page. At the top, a note says 'The scan repeat interval is determined automatically.' Below this, there are two sections: 'URL of list of authorized access points' with a 'Test List URL...' button, and 'Repeat scan every: 600 seconds' with a 'Save' button. Below these are two tables: 'Unauthorized access points' and 'All access points'. Both tables have columns for MAC address, SSID, Status, Mode, Channel, Signal, Noise, SNR, and Info. Under 'XML version', there are links for 'Detailed' and 'Brief' XML output. A note at the bottom right of the tables states '* Frequency used by this access point'.

Unauthorized access points								
MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info
XML version: Detailed Brief								

All access points								
MAC address	SSID	Status	Mode	Channel	Signal	Noise	SNR	Info
XML version: Detailed Brief								

Figure 6-5: Wireless Neighborhood

NOTE



If a AP is not broadcasting its name, the corresponding SSID column is empty.

6.2.1 Scanning Frequency

Scanning frequency depends on how the radio is configured.

Scanning is performed automatically if you defined any of the following on the **Wireless > Radio(s)** configuration page:

- Operating mode is set to Monitor and, on this Wireless neighborhood page,
- Repeat scan every is enabled.
- Channel is set to Automatic.
- Automatic power control is enabled.

The scanning interval is set based on the automatic power control and channel selection intervals that are defined.

In the case of Monitor mode, scanning is continuous, switching channels each 200 ms. If none of these options is defined, you must set the scanning interval manually.

Scanning is temporarily disabled when a Network trace is active.

Each time a scan is repeated, it moves up one channel in the range supported by the current wireless mode (a/b/g). To view a list of all APs operating on all channels, you must perform multiple scans. Define Repeat scan every accordingly. The results of each scan are shown in the All APs list.

When operating in Monitor mode, the AP scans all channels and all wireless modes (a/b/g). Scanning is automatically performed on all active radios.

To identify unauthorized APs, the AP compares the MAC address of each discovered AP against the list of authorized APs—which you must define. If the discovered AP does not appear in the list, it is shown in the Unauthorized APs list.

6.2.2 Identifying Unauthorized APs

Improperly configured wireless APs can seriously compromise the security of a corporate network. It is therefore important that these APs be identified as quickly as possible.

You can configure the wireless neighborhood feature to automatically list all unauthorized APs that are operating nearby.

To identify unauthorized APs, the network neighborhood feature compares the MAC address of each discovered AP against the list of authorized APs that you have defined as discussed below. If the discovered AP does not appear in the list, its name is shown in the **Unauthorized access points** list.

The list of authorized APs file is in XML format. Each entry in the file comprises two items: MAC address and SSID. Each entry should appear on a new line. The easiest way to create this file is to wait for a scan to complete, then open the list of all APs in **Brief** format. Edit this list so that it contains only authorized AP and save it. Then specify the address of this file under **List of authorized access points**.

You must edit the **Brief** list file to remove extra text that appears before and after each MAC address. For example, if the brief list appears as follows

```
<?xml version='1.0'?> <simple-ap-list> # MAC  SSID  
00:03:52:07:f5:11 "AP_1"  
00:03:52:07:f5:23 "AP_2"  
00:03:52:07:f5:12 "AP_3"  
</simple-ap-list>
```

reformat the list to appear as follows

```
00:03:52:07:f5:11 "AP_1"  
00:03:52:07:f5:23 "AP_2"  
00:03:52:07:f5:12 "AP_3"
```

6.3 Radio Configuration

To define configuration settings for the radio, select **Wireless > Radio(s)**. This opens the Radio(s) configuration page (example from Wi² AP shown):

Left Screenshot (Operating mode: Access point and Local mesh):

- Regulatory domain: UNITED STATES
- Operating mode: Access point and Local mesh
- Wireless mode: 802.11b + 802.11g
- Channel: Automatic
- Interval: Disabled
- Time of day: 00 : 00 : mm
- Currently: Channel 1, 2.412GHz
- Automatic channel exclusion list: Channel 1, 2.412GHz; Channel 2, 2.417GHz; Channel 3, 2.422GHz
- Distance between access points: Large
- RTS threshold: bytes
- Multicast Tx rate: 1.0 Mb/s
- Antenna selection: Diversity (both antennas)
- Beacon interval: 100 time units (TU)
- Spectralink VIEW:
- Maximum range (ack timeout): 0-1 km

Right Screenshot (Operating mode: Monitor):

- Regulatory domain: UNITED STATES
- Operating mode: Monitor
- Wireless mode: 802.11b + 802.11g
- Channel: Automatic

Transmit power control:

- Maximum available output power:
- 10 dBm = 10 % of max output power
- Automatic power control:
- Interval: 1 hour

Maximum output power: 20 dBm

Figure 6-6: Radio Configuration

6.3.1 Configuration Parameters

NOTE



If multiple radios are available on a AP, configuration options for each radio are the same.

6.3.1.1 Operating mode

Select the operating mode. Available options are:

- **Access point and Local mesh:** Standard operating mode provides support for all wireless functions.
- **Access point only:** Only provides AP functionality, local mesh links cannot be created.
- **Local mesh only:** Only provides local mesh functionality. Wireless client stations cannot connect.
- **Monitor:** Puts the radio in promiscuous mode (no transmissions). Both AP and local mesh functionality are disabled. Use this option for continuous scanning across all channels in all wireless modes (a/b/g). See the results of the scans on the **Wireless > Neighborhood page**.
- This mode also enables 802.11 traffic to be traced when using the **Tools > Network** trace command.

6.3.1.2 Wireless Mode

Select the transmission speed and frequency band:

- 802.11b: 11 Mbps in the 2.4 GHz frequency band.
- 802.11b + 802.11g: 11 and 54 Mbps in the 2.4 GHz frequency band.
- 802.11g: 54 Mbps in the 2.4 GHz frequency band.

6.3.1.3 Channel

Select channel and frequency for wireless services. The channels that are available are determined by the radio installed in the AP and the regulations that apply in your country.

Use the **Automatic** option to have the AP select the best available channel.

If setting the channel manually, for optimal performance when operating in 802.11b or 802.11g modes, select a channel that differs from other wireless APs operating in neighboring cells by at least 25 MHz. Consult the **Wireless > Neighborhood** page to view a list of APs currently operating in your area.

6.3.1.4 Interval

When the Automatic option is selected for Channel, this parameter determines how often the AP re-evaluates the channel setting. Select Time of day to have the channel setting re-evaluated at a specific time of day.

6.3.1.5 Time of Day

When the Time of Day option is selected for Interval, this parameter determines the time of day that the AP re-evaluates the channel setting. Set hours in the range 0 to 23.

6.3.1.6 Automatic Channel Exclusion List

Used when **Automatic** is selected under **Channel**, this parameter determines the channels that are not available for automatic selection. To select more than one channel, hold down CTRL as you select the channel names.

6.3.1.7 Distance Between Access Points

(Not available in Monitor mode)

Use this parameter to adjust the receiver sensitivity of the AP only if:

- You have more than one wireless AP installed in your location.
- You are experiencing throughput problems.

In all other cases use the default setting of Large.

If you have installed multiple APs, reducing this AP's receiver sensitivity:

- Helps to reduce the amount of cross-talk between the wireless stations to better support roaming clients
- Increases the probability that client stations connect with the nearest AP

6.3.1.7.1 Available settings

- Large: Accepts all clients.

- Medium: Accepts clients with an RSSI greater than 15 dB.
- Small: Accepts clients with an RSSI greater than 20 dB.

NOTE

RSSI (Received Signal Strength Indication) is the difference between the amount of noise in an environment and the wireless signal strength. It is expressed in decibels (dB). The higher the number the stronger the signal.

6.3.1.7.2 RTS Threshold

(Not available in Monitor mode)

Use this parameter to control collisions on the link that can reduce throughput. If the **Status > Wireless** page shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated. Note that using a small value for RTS threshold can affect throughput. Range is 128 to 1540.

If a packet is larger than the threshold, the AP will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the AP send the packet. Packets smaller than the threshold are transmitted without this handshake.

6.3.1.7.3 Multicast Tx Rate

(Not available in Monitor mode)

Use this parameter to set the transmit rate for multicast traffic. This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, the multicast is not seen by the station.

6.3.1.7.4 Antenna Selection

(Not available in Monitor mode)

Select the antenna the radio will transmit and receive on. Regardless of the antenna that is selected, the AP can only create a single wireless cell using the radio.

- If a single antenna is used, it can be connected to either Main or Aux.
- When creating a point-to-point wireless bridge, it is recommended that a single directional antenna be used on either Main or Aux.

- For maximum wireless coverage, use two omnidirectional antennas, and select the Diversity option.

6.3.1.7.5 Beacon Interval

(Not available in Monitor mode)

Sets the number of time units (TUs) that the AP waits between transmissions of the wireless beacon. One TU equals 1024 microseconds. The default interval is 100 TU, which is equal to 102.4 milliseconds. Supported range is from 20 to 500 TU.

6.3.1.7.6 Spectralink VIEW

(Not available in Monitor mode)

Provides support for Spectralink phones using Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) extensions.

6.3.1.7.7 Maximum Range (Ack Timeout)

Fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, timeout is optimized for links of less than 1 km.

NOTE



This is a global setting that applies to all wireless connection made with the radio. Therefore, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

6.3.1.7.8 Transmit Power Control

(Not available in Monitor mode)

Use this parameter to set the transmission power of the wireless radio. The maximum supported power setting depends on the radio that is installed. The actual **Maximum output power** is shown at the bottom of this group box.

Select the **Maximum available output power** checkbox to specify that the AP use maximum available power. Alternatively, you can enter transmission power in dBm (using a range between 0 and 20, even though not all radios can support up to 20 dBm), or as a percentage of the maximum available power (using a range between 0 and 100).

Actual transmit power used may be less than the specified value. The AP determines the power to be used based on the settings you make for regulatory domain, wireless mode, and operating frequency.

Select **Automatic power control** to enable the AP to determine the optimal power setting within the defined limits. Also select the Interval at which power is adjusted. (Interval is relevant only if **Automatic power control** is selected.).

NOTE



If the **Automatic power control** option is enabled, the AP may dynamically change the **Minimum rate** configured in all Virtual Network profiles. This is done to maintain a reasonable connection speed for client stations when the AP is operating in environments with strong interference.

This feature works best when the entire network uses only Alvarion Ltd. APs, because third-party products will not adjust output power.

If co-channel interference is discovered, all neighboring APs will shrink their cell size to minimize the interference. The first step is to adjust the transmit power. If this fails, the next step is to increase transmit power to maximum, if possible, and to change the minimum data rate to a higher value. 802.11b will change from 1 Mbps to 2 Mbps, 802.11g will change from 6 Mbps up to 18 Mbps.

NOTE



Not all interference can be eliminated, as a majority of clients will still transmit at maximum power.

NOTE



Some older wireless client cards may not support a data rate of 2 Mbps and therefore may not be able to associate when Automatic power control is enabled.

Chapter 7 - Network Configuration

In This Chapter:

- “Port Configuration” on page 108
- “VLAN Support” on page 112
- “Bandwidth Control” on page 116
- “CDP” on page 117
- “DNS” on page 118
- “IP Routes” on page 120
- “IP QoS” on page 122

7.1 Port Configuration

The **Port configuration** page displays summary information about all logical and physical ports and VLANs. Open this page by selecting **Network > Ports**.

The screenshot shows two stacked tables. The top table is titled 'Port configuration' and lists three ports: 'Bridge port', 'Wireless port', and 'Port 1'. Each row includes a status icon (green circle for Bridge port, green circle for Wireless port, green circle with a cloud for Port 1), the port name, its IP address (192.168.1.55 for Bridge port, [bridged] for others), its subnet mask (255.255.255.0 for Bridge port, [bridged] for others), and its MAC address (00:10:E7:02:42:E0 for Bridge port, 00:10:E7:02:42:E0 for Wireless port, 00:10:E7:02:48:CC for Port 1). The bottom table is titled 'VLAN configuration' and has columns for Name, Port, VLAN, IP address, and Mask. It contains one entry: 'Add New VLAN...'.

Port configuration				
Jack	Name	IP address	Mask	MAC address
●	Bridge port	192.168.1.55	255.255.255.0	00:10:E7:02:42:E0
●	Wireless port	[bridged]	[bridged]	00:10:E7:02:42:E0
●	Port 1	[bridged]	[bridged]	00:10:E7:02:48:CC

VLAN configuration				
Name	Port	VLAN	IP address	Mask
Add New VLAN...				

Figure 7-1: Port Configuration

7.1.1 Port Configuration Information

- **Status indicator:** Operational state of each port, as follows:
 - » **Green:** Port is properly configured and ready to send and receive data.
 - » **Red:** Port is not properly configured, disabled, or disconnected.
- **Jack:** Physical interface to which a logical port is assigned.
- **Name:** Identifier for the port. To configure a port, click its name.
- **IP address:** IP addresses assigned to the port. An address of **0.0.0.0** means that no address is assigned.
- **Mask:** Subnet mask for the IP address.
- **MAC address:** MAC address of the port.

7.1.2 Bridge Port Configuration

All ports on the AP are bridged. Therefore, common settings are configured using the bridge port (which is a logical port). To verify and possibly adjust bridge port configuration, select **Network > Ports > Bridge port**.

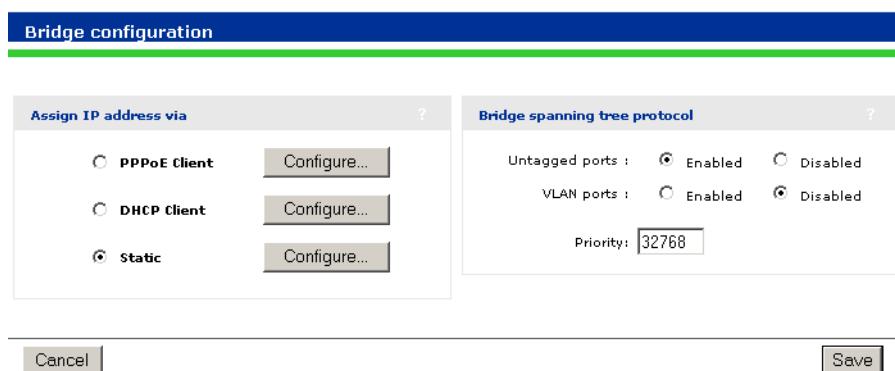


Figure 7-2: Bridge Configuration

7.1.2.1 Assigning an IP Address

The bridge port supports the following addressing options:

- PPPoE client
- DHCP client (default setting)
- Static

By default, the bridge port operates as a DHCP client. Select the addressing option that is required by your network administrator and then select **Configure**. Refer to the online help for descriptions of all configuration options.

7.1.2.2 Bridge Spanning Tree Protocol

When this option is enabled, the AP uses the Spanning-Tree Protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

Spanning tree can be enabled for untagged ports and/or VLAN ports.

When VLAN support is enabled, it applies to VLANs defined on the **Network > Ports** page only. It does not apply to the management VLAN defined in the VLAN box on the **Network > Ports > Port 1** or **Port 2** page.

7.1.2.2.1 Priority

Sets the priority of the AP within the spanning tree network. Generally, the bridge with lowest priority is designated as the root bridge of the spanning tree.

7.1.3 Port Configuration

To verify and possibly adjust port configuration, select **Network > Ports > Port n**. Configuration options for both ports are the same.

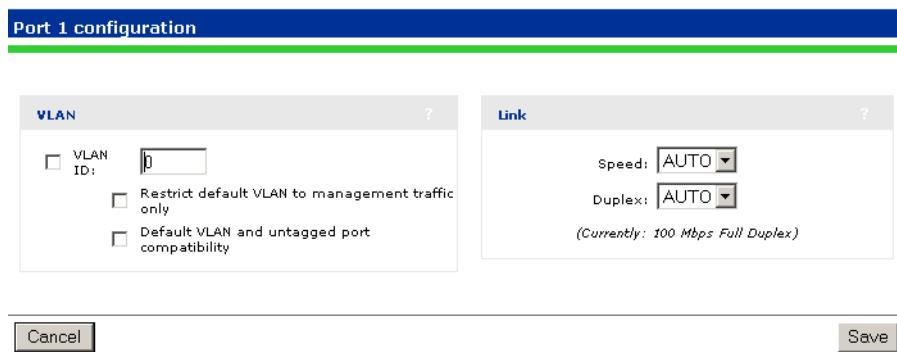


Figure 7-3: Port 1 Configuration

7.1.3.1 VLAN

7.1.3.1.1 VLAN ID

Defines the default VLAN ID for this port. All outgoing traffic that does not have a VLAN already assigned to it, is sent on this VLAN.

NOTE



Do not assign this same VLAN ID to users dynamically via RADIUS. If you do, traffic for these users will be blocked.

7.1.3.1.2 Restrict Default VLAN to Management Traffic Only

The default VLAN can be restricted to carry management traffic only. Management traffic includes:

- All traffic that is exchanged with the access controller (login authentication requests/replies)
- All traffic that is exchanged with external RADIUS servers
- HTTPS sessions established by administrators to the management tool
- Incoming and outgoing SNMP traffic

- DNS requests and replies

7.1.3.1.3 Default VLAN and Untagged Port Compatibility

When this option is enabled, any traffic being sent on the default VLAN is also sent untagged on this port.

7.1.3.2 Link

7.1.3.2.1 Speed

- Auto: Lets the AP automatically set port speed based on the type of equipment it is connected to.
- 10: Forces the port to operate at 10 mbps.
- 100: Forces the port to operate at 100 mbps.

7.1.3.2.2 Duplex

- Auto: Lets the AP automatically set duplex mode based on the type of equipment it is connected to
- Full: Forces the port to operate in full duplex mode.
- Half: Forces the port to operate in half duplex mode.

7.1.4 Wireless Port Configuration

See “[Radio Configuration](#)” on page 100.

7.2 VLAN Support

The AP provides a robust and flexible virtual local area network (VLAN) implementation that supports a wide variety of scenarios.

For example, VLANs can be used to isolate management from user traffic, or to route traffic over a local mesh connection.

You can map user traffic to a VLAN for each virtual service community (VSC) or on a per-user basis by setting the appropriate RADIUS attributes in a user's account.

Up to 80 VLAN definitions can be created. VLAN ranges are supported enabling a single definition to span a range of VLAN IDs.

The following AP features can be supported on a VLAN:

- Management tool access
- SNMP access
- SOAP access

For examples that illustrate how to work with VLANs, see the *Deployment Guide*.

7.2.1 Using a Default VLAN

You can configure port 1 or port 2 with a default VLAN setting so that any outgoing traffic that is not tagged with a VLAN ID receives the default ID.

You can restrict this default VLAN to carry management traffic only, which includes the following:

- All traffic that is exchanged with the access controller (login authentication requests/replies)
- All traffic that is exchanged with external RADIUS servers
- HTTPS sessions established by administrators to the management tool
- Incoming and outgoing SNMP traffic
- DNS requests and replies

To assign a default VLAN, see “[Port Configuration](#)” on page 110.

7.2.2 Assigning Traffic to a VLAN

You can assign wireless traffic to a VLAN for an entire Virtual Network or for individual users.

NOTE



A VLAN that is assigned to a user overrides a VLAN assigned by a Virtual Network or by the default VLAN.

7.2.2.1 Assigning a VLAN to a Virtual Network

You can map each virtual network to its own VLAN. Wireless clients that connect to a Virtual Network with VLAN support are bridged to the appropriate VLAN. Address allocation and security measures are the responsibility of the target network to which the VLAN connects.

NOTE



You cannot assign the same VLAN ID to the default VLAN and to a VLAN that is mapped to a virtual service community.

For information on how to assign a VLAN to a virtual network, see “[Egress VLAN](#)” on page 73.

7.2.2.2 Assigning VLANs to Individual Users

You can assign a VLAN to an individual user by setting attributes in the user’s RADIUS account. Restrictions are as follows:

- A user cannot be assigned to a VLAN that is set as the default VLAN on port 1 or port 2.
- A user can only be assigned to a predefined VLAN.
- MAC authentication does not support this feature; it can be used only for 802.1x client stations.

For more information see “[Configuring User Profiles on a RADIUS Server](#)” on page 147.

7.2.3 VLAN Bridging

If you assign a VLAN ID to more than one interface, the VLAN is bridged across the interfaces.

For example, if you create the VLANs shown in the following table, all VLAN traffic with ID 50 is bridged across all these interfaces. If you create a Virtual Network and assign the egress VLAN to any of these VLANs, output from the virtual network can be sent to any interface.

VLAN name	VLAN ID	Assigned to
Bridge_1	50	Port 1
Bridge_2	50	Port 2
Bridge_3	50	Local mesh 1

7.2.4 VLAN Configuration

To view and configure VLAN definitions, select **Network > Ports** and look in the **VLAN configuration** box:

Name	Port	VLAN	IP address	Mask
Bridge_1		50		
Bridge_2		50		
Bridge_3		50		

[Add New VLAN...](#)

Figure 7-4: VLAN Configuration

To add a VLAN, click **Add New VLAN**. The **Add/Edit VLAN** page opens.

General	
Port:	Port1
VLAN ID:	<input type="text"/>
VLAN name:	<input type="text"/>
Assign IP address via	
<input checked="" type="radio"/> DHCP client <input type="radio"/> Static <input type="radio"/> None	
IP address:	<input type="text"/>
Mask:	<input type="text"/>

[Cancel](#) [Save](#)

Figure 7-5: Adding A VLAN

Define VLAN settings as described in the following sections.

7.2.4.1 General

- **Port:** Select the physical interface with which the VLAN is associated.
- **VLAN ID:** Specify a VLAN identifier. If the VLAN is assigned to port 1 or port 2, you can also define a range of VLANs in the form *X-Y*, where *X* and *Y* can be 1 to 4094; for example, *50-60*. This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can define more than one VLAN range, but each range must be distinct.

NOTE



VLANs with ranges cannot be used for **Virtual Network egress mapping** and cannot be assigned an IP address.

- **VLAN name:** Specify a name to identify the VLAN definition on the AP. This name has no operational significance.

7.2.4.2 Assign IP Address Via

Specify how the VLAN obtains an IP address, as follows:

- **DHCP client:** Available only on VLANs that are assigned to port 1 or port 2. The VLAN obtains its IP address from a DHCP server on the same VLAN.
- There is no support for obtaining a default gateway from the DHCP server.
- **Static:** Enables you to manually assign an IP address to the VLAN. If you select this option, you must specify a static **IP address**, **Mask**, and **Gateway**.
- **None:** Specifies that this VLAN has no IP address. Use this option when the VLAN ID is defined as a range.

7.3 Bandwidth Control

The AP incorporates a bandwidth management feature that provides control of outgoing user traffic on the wireless ports.

To configure Bandwidth control, select **Network > Bandwidth control**.

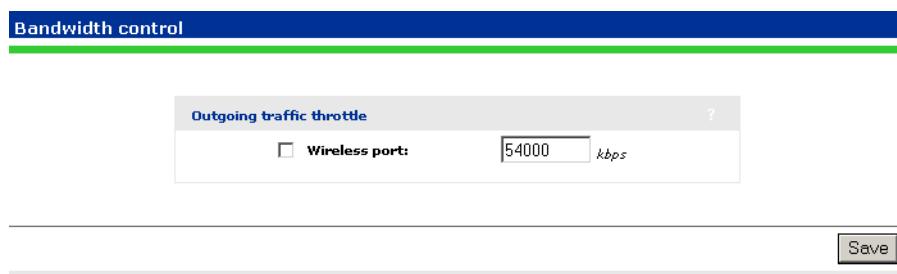


Figure 7-6: Bandwidth Control

- If outgoing traffic arrives at the defined bandwidth limit (or less), it is processed without delay.
- If outgoing traffic arrives at a rate that is greater than the defined bandwidth limit, it causes the AP to throttle the traffic. If the traffic rate is over-limit for just a short burst, the data will be queued and forwarded without loss. If the traffic rate is over-limit for a sustained period, the AP will drop data to bring the rate down to the bandwidth limit that is set.

For example, if you set bandwidth control to 5000 kbps, the maximum traffic that can be sent to client stations on each wireless port is 5000 kbps.

7.4 CDP

The AP can be configured to transmit CDP (Cisco Discovery Protocol) information on all ports. This information is used to advertise AP information to third-party devices, such as CDP-aware switches.

When installed with a service controller, the service controller uses CDP information sent by autonomous APs to collect information about these APs for display in its management tool.

To enable CDP transmission, select **Network > CDP**.

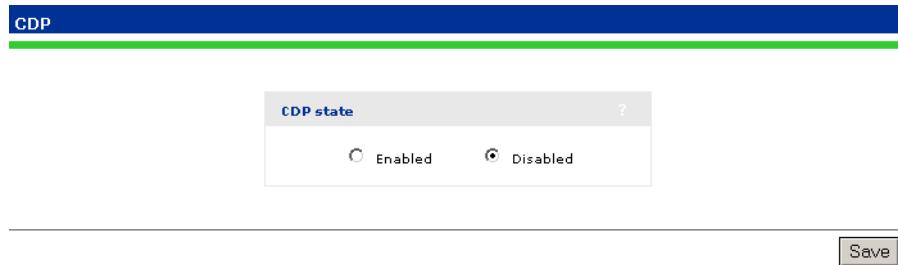


Figure 7-7: CDP

7.5 DNS

The AP provides several options to customize DNS handling. To configure these options, select **Network > DNS**.

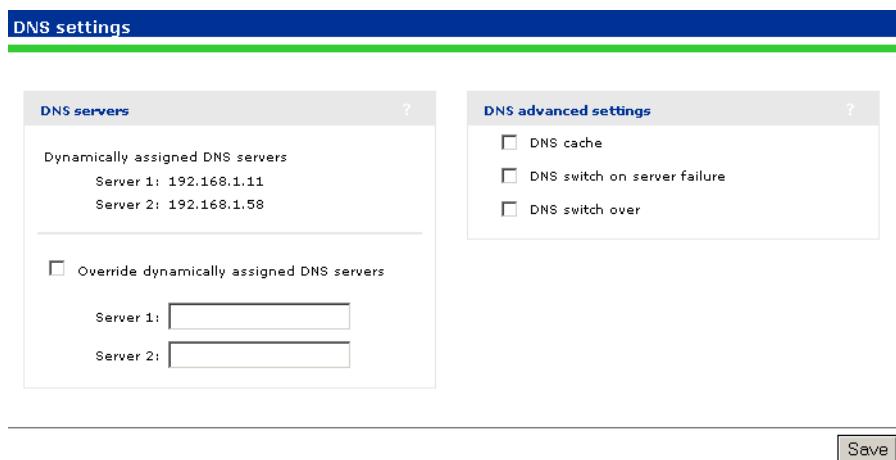


Figure 7-8: DNS

7.5.1 DNS Servers

- **Server 1:** Specify the IP address of the primary DNS server for the AP to use.
- **Server 2:** Specify the IP address of the secondary DNS server for the AP to use.

7.5.2 DNS Advanced Settings

7.5.2.1 DNS Cache

Enable this checkbox to activate the DNS cache. Once a host name is successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, because the remote DNS server does not have to be queried for subsequent requests for this host.

An entry stays in the cache until one of the following is true:

- An error occurs when connecting to the remote host
- The time to live (TTL) of the DNS request expires
- The AP restarts

7.5.2.2 DNS Switch on Server Failure

This setting controls how the AP switches between the primary and secondary DNS servers.

- When enabled, the AP switches servers if the current server replies with a DNS server failure message.
- When disabled, the AP switches servers if the current does not reply to a DNS request.

7.5.2.3 DNS Switch Over

This setting controls how the AP switches back to the primary DNS server after it has switched to the secondary DNS server because the primary was unavailable.

- When enabled, the AP switches back to the primary server after it becomes available again.
- When disabled, the AP switches back to the primary server only if the secondary server becomes unavailable.

7.5.2.4 Logout Host Name

If a user that is logged in via HTML sends a DNS request for the specified host name, the AP will log the user out.

7.6 IP Routes

All wireless traffic on the AP is bridged to the egress interface on the virtual network with which it is associated. Therefore, IP routes cannot be applied to user traffic.

However, IP routes can be used to ensure that the management traffic generated by the AP is sent to the correct destination. For example, if two virtual networks are defined, each with authentication assigned to a different RADIUS server operating on a different subnet and VLAN, routing table entries may be required to ensure proper communication with the RADIUS servers.

7.6.1 Configuration

To view and configure IP routes, select **Network > IP routes**.

Active routes					
Interface	Destination	Mask	Gateway	Metric	Delete
Bridge port	192.168.1.0	255.255.255.0	*	0	
					Add

Default routes			
Interface	Gateway	Metric	Delete
Bridge port	192.168.1.2	1	
			Add

Figure 7-9: IP Routes

7.6.1.1 Active Routes

This table shows all active routes on the AP. You can add routes by specifying the appropriate parameters and then selecting **Add**.

The routing table is dynamic and is updated as needed. This means that during normal operation the AP adds routes to the table as required. You cannot delete these system routes.

The following information is shown for each active route:

- **Interface:** The port through which traffic is routed. When you add a route, the AP automatically determines the interface to be used based on the **Gateway** address.
- **Destination:** Traffic addressed to this IP address is routed.

- **Mask:** Number of bits in the destination address that are checked for a match.
- **Gateway:** IP address of the gateway to which the AP forwards routed traffic (known as the next hop).
- An asterisk is used by system routes to indicate a directly connected network.
- **Metric:** Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric.

7.6.1.2 Default Routes

The **Default routes** table shows all default routes on the AP. Default routes are used when traffic does not match any route in the Active routes table. You can add routes by specifying the appropriate parameters and then selecting **Add**.

The routing table is dynamic and is updated as needed. If more than one default route exists, the first route in the table is used.

The following information is shown for each default route:

- **Interface:** The port through which traffic is routed. When you add a route, the AP automatically determines the interface to be used based on the **Gateway** address.
- **Gateway:** IP address of the gateway to which the AP forwards routed traffic (known as the next hop).
- An asterisk is used by system routes to indicate a directly connected network.
- **Metric:** Priority of a route. If two routes exist for a destination address, the AP chooses the one with the lower metric.

7.7 IP QoS

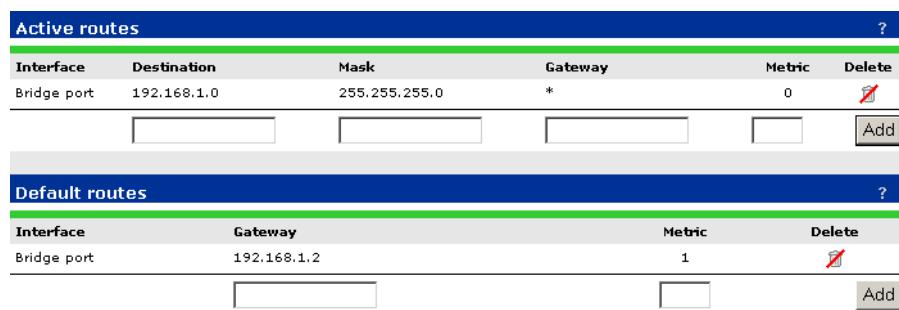
To ensure that critical applications have access to the required amount of wireless bandwidth, you can classify packets destined for the wireless interface into priority queues based on a number of criteria. For example, you can use any of the following to place data packets in one of four priority queues for transmission onto the wireless interface:

- TCP source port
- UDP source port
- Destination port
- Port ranges

You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with virtual networks or use for global wireless settings. You can configure as many as 32 IP QoS profiles on the AP. You can associate as many as 10 IP QoS profiles with each virtual network.

7.7.1 Configuration

To view and configure IP QoS profiles, select **Network > IP QoS**. Initially, no profiles are defined.



The screenshot shows two tables: "Active routes" and "Default routes".

Active routes

Interface	Destination	Mask	Gateway	Metric	Delete
Bridge port	192.168.1.0	255.255.255.0	*	0	

Default routes

Interface	Gateway	Metric	Delete
Bridge port	192.168.1.2	1	

Figure 7-10: IP QoS Profiles

To create an IP QoS profile select **Add New Profile**.

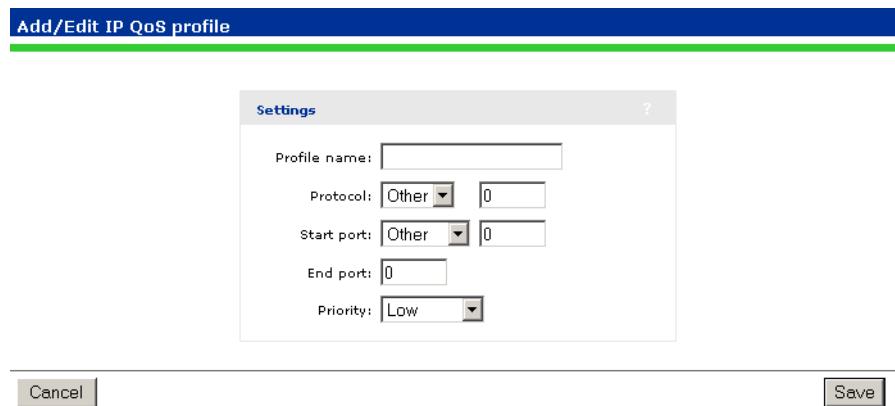


Figure 7-11: Adding a New IP QoS Profile- Priority: Low

7.7.1.1 Settings

- **Profile name:** Specify a unique name to identify the profile.
- **Protocol:** Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers at <http://www.iana.org>.
- **Start port/ End port:** Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port**. Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

NOTE



To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0**.

- **Priority:** Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

NOTE

It is strongly recommended that you reserve **Very high** priority for voice applications.

7.7.2 Example

This example shows how to create two IP QoS profiles and associate them with a Virtual Network. The two profiles are:

- **Voice:** Provides voice traffic with high priority.
- **Web:** Provides HTTP traffic with low priority.

7.7.2.1 Create the Profiles

- 1 Select **Network > IP QoS**, and then **Add New Profile**. The **IP QoS Profile** page opens.
- 2 Under **Profile name**, specify **Voice**.
- 3 Under **Protocol**, from the drop-down list select **TCP**.
- 4 Under **Start port**, from the drop-down list select **SIP**. **Start port** and **End port** are automatically populated with the correct value: **5060**.
- 5 Under **Priority**, from the drop-down list select **Very High**

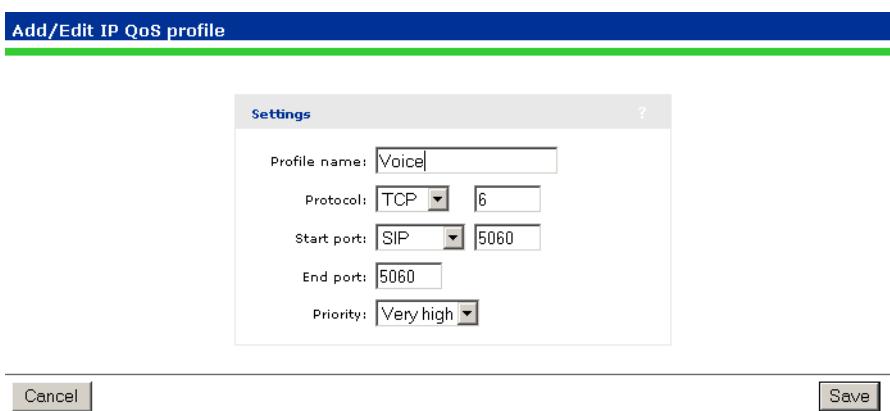


Figure 7-12: Adding a New IP QoS Profile- Priority: Very High

- 6 Select **Save**.

NOTE

You could also create another profile using the same parameters but for UDP to cope with any kind of SIP traffic.

- 7 On the **IP QoS Profile** page select **Add New Profile**.
- 8 Under **Profile name**, specify **Web**.
- 9 Under **Protocol**, from the drop-down list select **TCP**.
- 10 Under **Start port**, from the drop-down list select **http**. **Start port** and **End port** are automatically populated with the common HTTP port, **80**.
- 11 Under **Priority**, from the drop-down list select **Low**.

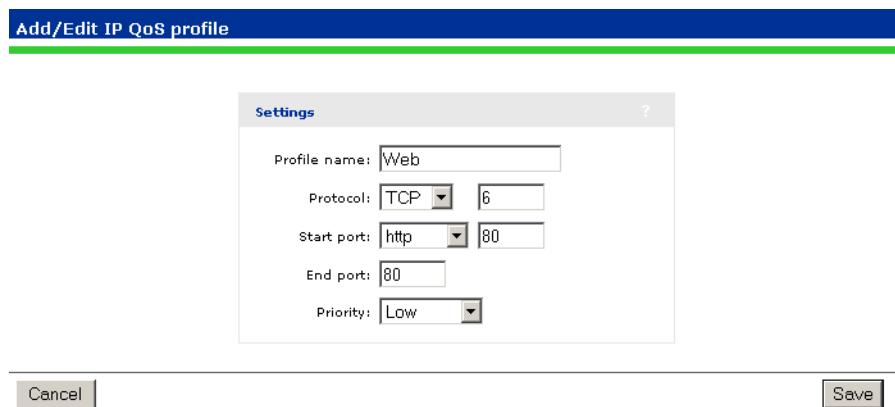


Figure 7-13: Adding a New IP QoS Profile- Profile Name: Web

- 12 Select **Save**.

7.7.2.2 Assign the Profiles to a Virtual Network

- 1 Select VSC on the main menu and then select one of the virtual network profiles in the **Name** column. Scroll down to the **Quality of service** section under **Virtual AP**.

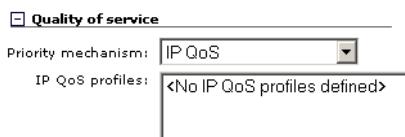
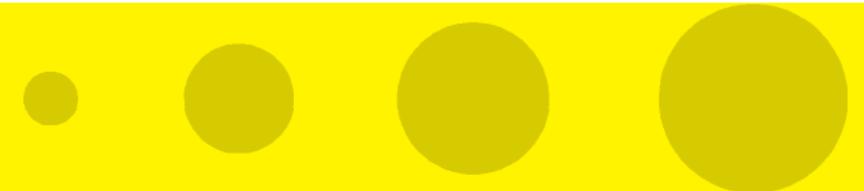


Figure 7-14: Quality of Service

- 2 Set **Priority mechanism** to **IP QoS**.

- 3 in **IP QoS profiles**, Ctrl-click each profile you want to add.
- 4 Select **Save**.



8

Chapter 8 - Management

In This Chapter:

- “Management Tool” on page 128
- “SNMP” on page 133
- “SOAP” on page 136
- “CLI” on page 138
- “System Time” on page 140
- “Country” on page 141

8.1 Management Tool

The management tool is a web-based interface to the AP that provides easy access to all configuration and monitoring functions.

8.1.1 Management Station

The *management station* refers to the computer that an administrator uses to connect to the management tool. To act as a management station, a computer must:

- Have a JavaScript-enabled web browser installed (at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0).
- Be able to establish an IP connection with the AP.

8.1.2 Starting the Management Tool

To launch the management tool, point your web browser to the IP address of the AP. By default, the address is 192.168.1.1.

For information on starting the management tool for the first time, see “[Configuration Procedure](#)” on page 53.

8.1.3 Customizing Management Tool Settings

To customize management tool settings, select **Management > Management tool**.

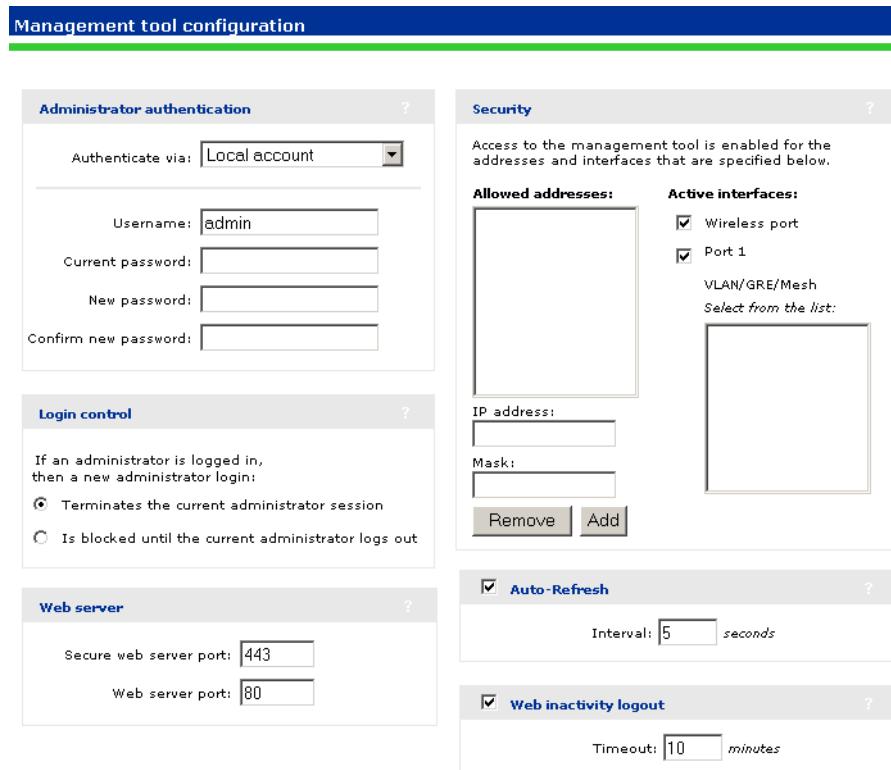


Figure 8-1: Management Tool Configuration

8.1.3.1 Administrator Authentication

Access to the management tool is protected by a username and password. The factory default setting for both is **admin**. It is recommended that you change both at initial setup, and then regularly thereafter.

CAUTION



If you forget the administrator password, the only way to access the management tool is to reset the AP to factory default settings. For information see “[Resetting to Factory Defaults](#)” on page 215.

8.1.3.2 Authenticating Administrators Using a RADIUS Server

The AP can be configured to use an external RADIUS server to authenticate administrators. One advantage of this method is that it enables several administrator accounts to be created, each with its own username and password.

Configure RADIUS authentication as follows:

- 1 Define an account for the administrator on the RADIUS server.
- 2 On the AP, create a RADIUS profile that will connect the AP to the RADIUS server. See “Configuring a RADIUS Client Profile on the AP” on page 144.
- 3 Under **Administrator authentication**, set **Authenticate via** to the RADIUS profile you created in step 2. In this example, the profile is called **Rad-1**.

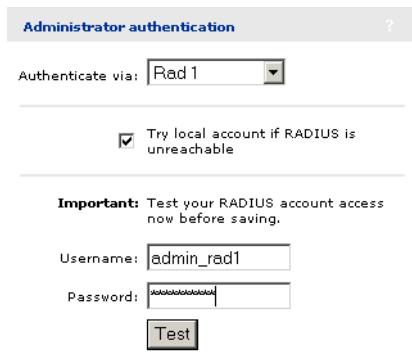


Figure 8-2: Administrator Authentication

- 4 Enable **Try local account if RADIUS unreachable**. This will allow you to login using the local account if the connection to the RADIUS server is unavailable.
- 5 It is recommended that before saving, you specify the **Username** and **Password** and select **Test** to ensure that the RADIUS server is reachable and that the administrator account is working properly.

CAUTION



If you do not enable the “Try local account if RADIUS unreachable option” and the service controller is unable to reach the RADIUS server, you will not be able to login.

8.1.3.3 Login Control

To maintain the integrity of the configuration settings, only one administrator can be connected to the management tool at a given time. To prevent the management tool from being locked by an idle administrator, two mechanisms are in place:

- If an administrator’s connection to the management tool remains idle for more than ten minutes, the AP automatically terminates the administrator’s session. You can configure this mechanism on the management tool configuration page.

- If a second administrator connects to the management tool and authenticates with the correct username and password, the first administrator's session terminates. You can configure this mechanism on the management tool configuration page.
- If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. This option is not configurable.

8.1.3.4 Web Server

You can also configure the web server ports from which access to the management tool is permitted.

- **Secure web server port:** Specify a port number for the AP to use to provide secure HTTPS access to the management tool. Default is 443.
- **Web server port:** Specify a port number for the AP to use to provide standard HTTP access to the management tool. These connections are met with a warning, and the browser is redirected to the secure web server port. Default is 80.

8.1.3.5 Security

The management tool is protected by the following security features:

- **HTTPS:** Communications between a management station and the AP is protected using the Secure Hypertext Transport Protocol. Before logging on to the management tool, you must accept a security certificate. A default certificate is provided with the service controller. You can replace this certificate with your own. For more information, see [“Managing Certificates” on page 155](#).
- **Port blocking:** You can enable or disable access to the management tool for each of the following:
 - » LAN port
 - » Internet port
 - » VPN

» VLAN/GRE/Mesh

- **Allowed IP address:** You can configure a list of subnets from which access to the management tool is permitted.

NOTE



These security settings also apply when SSH is used to access the command line interface.

8.1.3.6 Auto-refresh

This option controls how often the AP updates the information in group boxes that show the auto-refresh icon in their title bar. Under **Interval**, specify the number of seconds between refreshes.

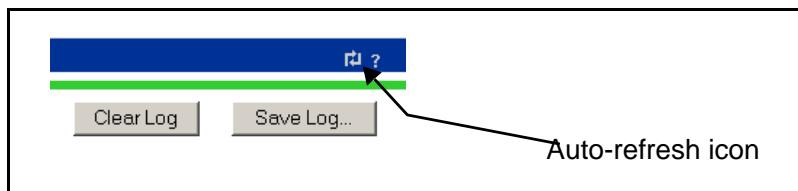


Figure 8-3: Auto-refresh Icon

8.1.3.7 Web Inactivity Logout

When this option is enabled, an administrator will automatically be logged out if their session is idle for the specified number of minutes.

8.2 SNMP

The AP provides a robust SNMP implementation supporting both industry standard and Alvarion-specific MIBs. For complete information on supported MIBs, see the *SNMP MIB Reference Guide*.

8.2.1 Configuring SNMP Settings

Select **Management > SNMP** to open the **SNMP configuration** page. This page enables you to configure SNMP attributes, agents, traps, and security.

The screenshot shows the 'SNMP configuration' page with the following sections:

- Attributes:**
 - System name: A733008420
 - Location: (empty)
 - Contact: (empty)
 - Community name: *****
 - Confirm community name: *****
 - Read-only name: *****
 - Confirm read-only name: *****
- Agent:**
 - Port: 161 UDP
 - SNMP Protocol: Version 2c
- Traps:**
 - Community name: (empty)
 - Trap destinations:
 - Host: (empty)
 - Port: 162
 - Buttons: Remove, Add
 - Configure Traps...
- Security:**
 - Access to the management tool is enabled for the addresses and interfaces that are specified below.
 - Allowed addresses:** (Empty list)
 - Active interfaces:**
 - Wireless port (unchecked)
 - Port 1 (checked)
 - VLAN/GRE/Mesh
 - Select from the list: (Empty list)
 - IP address: (empty)
 - Mask: (empty)
 - Buttons: Remove, Add

At the bottom right is a 'Save' button.

Figure 8-4: SNMP Configuration

8.2.1.1 Attributes

- **System name:** Specify a name to identify the AP. Default is the AP's serial number.
- **Location:** Specify a descriptive name for the location where the AP is installed.
- **Contact:** Specify information about a contact person for the AP.
- **Community name:** Specify the password that controls read/write access to SNMP information. A network management program must supply this password when attempting to **set** or **get** SNMP information from the AP. By default, this is set to **private**.
- **Confirm community name:** Reenter the **Community name**.
- **Read-only name:** Specify the password that controls read-only access to the SNMP information. A network management program must supply this password when attempting to **get** SNMP information from the AP. By default the **Read-only name** is **public**.
- **Confirm read-only name:** Reenter the **Read-only name**.

8.2.1.2 Agent

The SNMP agent is active by default. If you disable the agent the AP will not respond to SNMP requests.

- **Port:** UDP port and protocol the AP uses to respond to SNMP requests. Default port is 161.
- **SNMP Protocol:** SNMP version supported. Default is **Version 2c** which also supports requests from agents using version 1.

8.2.1.3 Security

Use these settings to control access to the SNMP interface.

- **Allowed addresses:** List of IP address from which access to the SNMP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add**.
- When the list is empty, access is permitted from any IP address.

- **Active interfaces:** Enable the checkboxes that correspond to the interfaces from which to allow access to the SNMP interface.

8.2.1.4 Traps

When this feature is enabled, the AP sends traps to the hosts that appear in the **Traps destinations** list.

The AP supports the following MIB II traps:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the AP supports a number of Alvarion-specific traps. Select **Configure Traps**. For a descriptions of these traps, see the online help.

8.3 SOAP

The AP provides a SOAP interface that can be used by SOAP-compliant client applications to perform configuration and management tasks.

8.3.1 Configuring the SOAP Server

Select **Management > SOAP** to open the **SOAP server configuration** page. By default, the SOAP server is enabled.

The screenshot shows the 'SOAP server configuration' page with two main sections: 'Server settings' and 'Security'.

Server settings:

- Secure HTTP (SSL/TLS)
- Using client certificate
- HTTP authentication
- Username: []
- Password: []
- Confirm password: []
- TCP port: 448

Security:

Access to the SOAP interface is enabled for the addresses and interfaces that are specified below.

Allowed addresses: [Empty list box]

Active interfaces:

- Wireless port
- Port 1
- VLAN/GRE/Mesh
Select from the list: [Empty list box]

IP address: []
Mask: []

Buttons: Remove, Add, Save

Figure 8-5: SOAP Server Configuration

8.3.1.1 Server Settings

8.3.1.1.1 Secure HTTP (SSL/TLS)

Enable this option to configure the SOAP server for SSL/TLS mode. When enabled, the Secure Sockets Layer (SSL) protocol must be used to access the SOAP interface.

8.3.1.1.2 Using client certificate

When enabled, the use of a X.509 client certificate is mandatory for SOAP clients.

8.3.1.1.3 HTTP authentication

When enabled, access to the SOAP interface is available via HTTP with the specified username and password.

8.3.1.1.4 TCP Port

Specify the number of the TCP port that SOAP uses to communicate with remote applications. Default is 448.

8.3.1.2 Security

Use these settings to control access to the SOAP interface.

- **Allowed addresses:** List of IP address from which access to the SOAP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add**.
- When the list is empty, access is permitted from any IP address.
- **Active interfaces:** Enable the checkboxes that correspond to the interfaces from which to allow access to the SOAP interface.

8.3.1.3 Security Considerations

- The SOAP server is configured for SSL/TLS mode, and the use of a X.509 client certificate is mandatory for SOAP clients.
- The SOAP server is configured to trust all client certificates signed by the default Alvarion SOAP CA installed on the AP.
- Users should generate and install their own SOAP CA private key/public key certificate to protect their devices from unauthorized access. This is important because the default SOAP CA and a valid client certificate are provided as an example to all customers. (See “[Managing Certificates](#)” on page 155.)

8.4 CLI

The AP provides a command line interface that can be used to perform configuration and management tasks via the serial port or an IP connection on any of the AP's interfaces.

For complete information using on the CLI, see the *AP CLI Reference Guide*.

A maximum of three concurrent CLI sessions are supported regardless of the connection type.

8.4.1 Configuring CLI Support

Select **Management > CLI** to open the **Command Line Interface (CLI) configuration** page.

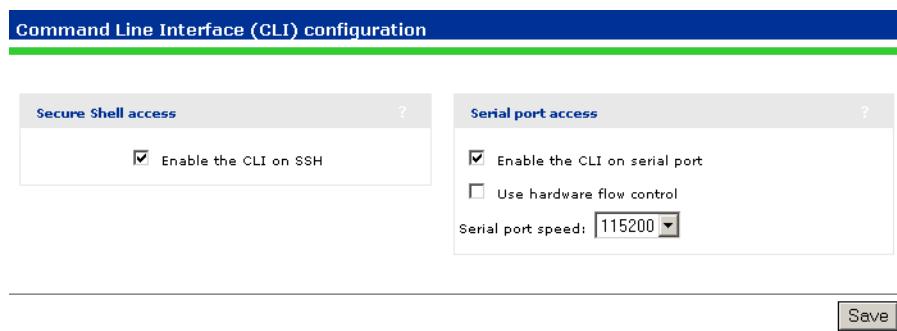


Figure 8-6: Command Line Interface (CLI) Configuration

8.4.1.1 Secure Shell Access

Enable this option to allow access to the CLI via an SSH session. The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for management tool administrators on the **Management > Management tool** page

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security**.
- The login credentials for SSH connections are the same as those defined under **Administrator authentication**.

NOTE

SSH logins always use the local administrator username and password, even if **Administrator authentication** is set to use an external RADIUS server.

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

8.5 System Time

Select **Management > System time** to open the **System time** page. This page enables you to configure the time server and time zone information.

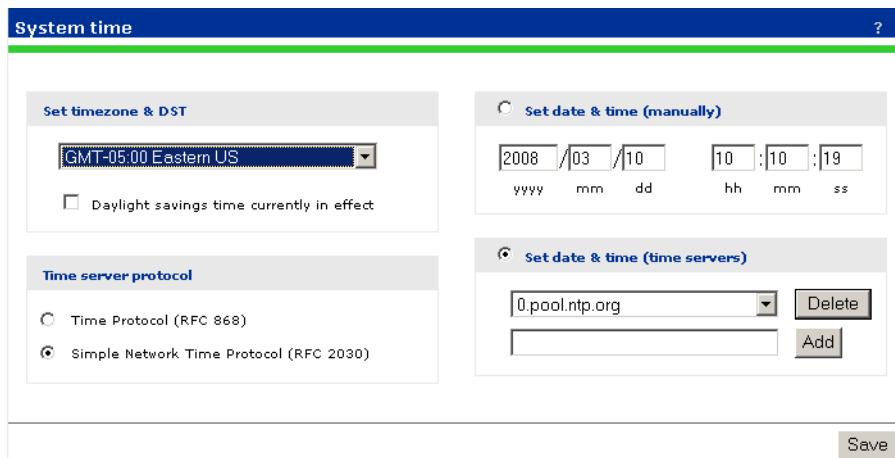


Figure 8-7: System Time

- 1 Set **timezone & DST** as appropriate.
- 2 Set **Time server protocol**, to **Simple Network Time Protocol**.
- 3 Select **set date & time (time servers)** and then select the desired time server. **Add** other servers if desired. The AP contacts the first server in the list. If the server does not reply, the AP tries the next server and so on.
- 4 Select **Save** and verify that the date and time is updated accurately. A working Internet connection on the AP Internet port is required.

NOTE



If you do not yet have an Internet connection on the AP Internet port, you can temporarily set the time manually with the **Set date & time (manually)** option. However, it is important to configure a reliable time server on the AP.

8.6 Country

NOTE



The Country sub-menu is not available on APs delivered with a fixed country setting. The country for which the AP is configured to operate is displayed on the management tool home page.

Select **Management > Country** and select the desired country.

CAUTION



Do not change Country to a country other than the one in which the AP operates. Failing to heed this caution may violate the regulatory compliance of the AP and engage your responsibility/liability for operating in your country.

Chapter 9 - Security

In This Chapter:

- “Using a RADIUS Server” on page 144
- “Managing Certificates” on page 155

9.1 Using a RADIUS Server

The AP can use one or more external RADIUS servers to perform a number of authentication and configuration tasks, including the tasks shown in the table below.

Task	For more information see
Validating administrator login credentials.	“Authenticating Administrators Using a RADIUS Server” on page 129
Validating user login credentials for 802.1X or MAC authentication types.	“Wireless Protection” on page 75 “MAC-based Authentication” on page 78
Storing custom configuration settings for each user.	“Configuring User Profiles on a RADIUS Server” on page 147
Storing accounting information for each user.	Accounting support is enabled under “Wireless Protection” on page 75 or “MAC-based Authentication” on page 78 .

9.1.1 Configuring a RADIUS Client Profile on the AP

The AP enables you to define a maximum of 16 RADIUS profiles. Each profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account on the RADIUS server. The settings for this account must match the profile settings you define on the AP.

For backup redundancy, each profile supports a primary and secondary server.

The AP can function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via authentication types such as: EAP-MD5, CHAP, MSCHAP v1/v2, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC.

9.1.1.1 Configuration Procedure

- 1 Select **Security > RADIUS profiles**. The RADIUS profiles page opens.

RADIUS profiles			
Name	Primary server	Secondary server	NAS ID
Rad_1	not configured	not configured	A733008420
Add New Profile...			

Figure 9-1: RADIUS Profiles

2 Select **Add New Profile**. The Add/Edit RADIUS Profile page opens.

Profile name	
Profile name:	<input type="text"/>

Primary RADIUS server	
Server address:	<input type="text"/>
Secret:	<input type="text"/>
Confirm secret:	<input type="text"/>

Settings	
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Retry interval:	<input type="text" value="10"/> seconds
<input type="checkbox"/> Retry timeout:	<input type="text" value="60"/> seconds
Authentication method:	<input checked="" type="checkbox"/> MSCHAPv2
<input type="checkbox"/> NAS ID:	<input type="text" value="A733008420"/>
<input type="checkbox"/> Always try primary server first	
<input checked="" type="checkbox"/> Use message authenticator	

Secondary RADIUS server (optional)	
Server address:	<input type="text"/>
Secret:	<input type="text"/>
Confirm secret:	<input type="text"/>

[Cancel](#) [Save](#)

Figure 9-2: Add/Edit RADIUS Profile

3 Configure the profile settings as described in the following Configuration Parameters section.

4 Select **Save**.

9.1.1.2 Configuration Parameters

9.1.1.2.1 Profile name

Specify a name to identify the profile.

9.1.1.2.2 Settings

- **Authentication port:** Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.

- **Accounting port:** Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.
- **Retry interval:** Specify the number of seconds that the RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the AP switches between the primary and secondary RADIUS servers, if a secondary server is defined. A reply that is received after the retry interval expires is ignored.

Retry interval applies to access and accounting requests that are generated by the following:

- » Administrator access to the management tool
- » MAC-based authentication of devices

You can determine the maximum number of retries as follows:

- » MAC-based authentication: Number of retries is infinite.
- » 802.1X authentication: Retries are controlled by the 802.1X client software.

- **Authentication method:** Select the default authentication method that the AP uses when exchanging authentication packets with the RADIUS server defined for this profile.

For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting.

If traffic between the AP and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS Server). PAP, MSCHAP V1, and CHAP are less secure protocols.

- **NAS ID:** Specify the identifier for the network access server that you want to use for the AP. By default the serial number of the AP is used. The AP includes the NAS-ID attribute in all packets that it sends to the RADIUS server.
- **Always try primary server first:** Enable this option if you want to force the AP to contact the primary server first.

Otherwise, the AP sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server if defined.

For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the AP sends the first RADIUS access request to the secondary RADIUS server.

If the secondary RADIUS server does not reply, the AP retransmits the RADIUS access request to the primary RADIUS server. When two servers are configured, the AP always alternates between the two.

- **Use message authenticator:** When enabled, causes the RADIUS Message-Authenticator attribute to be included in all RADIUS access requests sent by the AP.

NOTE



This option has no effect on IEEE802dot1x authentication requests. These requests always include the RADIUS Message-Authenticator attribute.

9.1.1.2.3 Primary/Secondary RADIUS Server

- **Server address:** Specify the IP address of the RADIUS server.
- **Secret/Confirm secret:** Specify the password for the AP to use to communicate with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server, proving that the packets originate from a valid/trusted source.

9.1.2 Configuring User Profiles on a RADIUS Server

You must create at least one user profile on the RADIUS server. You can associate multiple user accounts with a single RADIUS profile.

This section presents all supported RADIUS and Alvarion attributes that can be used to configure a user profile on a RADIUS server. Attributes starting with *MS* are Microsoft and are not standard.

NOTE

The attributes listed in this section are only supported on non-access controlled Virtual Networks (when the **Use Alvarion access controller** option is disabled in the VSC's **General** box). For attributes supported on access-controlled Virtual Networks, refer to the documentation for the Alvarion access controller.

NOTE

In the following definitions strings are defined as 1 to 253 characters long.

9.1.2.1 About Alvarion Ltd. Vendor-specific Attribute

The Alvarion Ltd. vendor-specific attribute conforms to RADIUS RFC 2865. You may need to define the Alvarion Ltd. vendor-specific attribute on your RADIUS server if it is not already present. You must specify the following:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type = string

9.1.2.2 Access Request Attributes

This table lists all attributes supported in Access Request packets for each authentication type.

Attribute	Admin login	802.1X	MAC	Format
Acct-Session-Id		■	■	32-bit unsigned integer
Called-Station-Id		■	■	Called-Station-Id
Calling-Station-Id		■	■	Calling-Station-Id
EAP-Message	■	■		EAP-Message
Framed-MTU	■	■		Framed-MTU
Message-Authenticator	■	■	■	Message-Authenticator
NAS-Identifier	■	■	■	NAS-Identifier
NAS-Ip-Address		■	■	NAS-Ip-Address
NAS-Port	■	■	■	NAS-Port
NAS-Port-Type	■	■	■	NAS-Port-Type

Attribute	Admin login	802.1X	MAC	Format
Service-Type	■	■	■	Service-Type
State	■	■		State
User-Name	■	■	■	User-Name
User-Password			■	User-Password
Alvarion-AVPair (SSID)			■	Alvarion-AVPair (SSID)

9.1.2.2.1 Descriptions

- **Acct-Session-Id** (32-bit unsigned integer): A unique accounting ID used to make it easy to match up records in a log file.
- **Called-Station-Id** (string): BSSID of the Virtual Network used by a wireless client, or the MAC address of the LAN port used by a wired client. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. This can be changed on the **Security > 802.1x** page.
- **Calling-Station-Id** (string): The MAC address of the 802.1x client station. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. This can be changed on the **Security > 802.1x** page.
- **Framed-MTU** (32-bit unsigned integer): Hard-coded value of 1496.
- **Message-Authenticator** (string): As defined in RFC 2869. Always present even when not doing an EAP authentication. Length = 16 bytes.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the RADIUS profile being used.
- **NAS-Ip-Address** (32-bit unsigned integer): The IP address of the port the AP is using to communicate with the RADIUS server.
- **NAS-Port** (32-bit unsigned integer): A virtual port number starting at 1. Assigned by the AP.
- **NAS-Port-Type** (32-bit unsigned integer): Always set to 19, which represents WIRELESS_802_11.)
- **Service-Type** (32-bit unsigned integer): Set to LOGIN_USER.
- **State** (string): As defined in RFC 2865.

- **User-Name** (string): The username assigned to the user. Or if MAC-authentication is enabled, the MAC address of the wireless client station.

The following attributes are mutually exclusive depending on the RADIUS authentication method.

- **User-Password** (string): The password supplied by a user or device when logging in. Encoded as defined in RFC 2865. Present only when the authentication scheme on the **Security > RADIUS > Profile 1** page is set to PAP/SecurID. Or if MAC-authentication is enabled, the MAC address of the wireless client station.
- **EAP-Message** (string): As defined in RFC 2869. Only present when the authentication scheme on the **Security > RADIUS > Profile 1** page is set to EAP-MD5.
- **Alvarion-AVPair** (SSID): See the description in the section that follows.

9.1.2.3 Access Accept Attributes

This table lists all attributes supported in Access Accept packets for each authentication type.

Attribute	Admin login	802.1X	MAC
Class		■	
EAP-Message		■	
MS-MPPE-Recv-Key		■	
MS-MPPE-Send-Key		■	
Session-TImeout		■	■
Termination-Action		■	■
Tunnel-Medium-Type		■	
Tunnel-Private-Group-ID		■	
Tunnel-Type		■	

9.1.2.3.1 Descriptions

- **Class** (string): As defined in RFC 2865. Multiple instances are supported.

- **EAP-Message** (string): Note that the content will not be read as the RADIUS Access Accept overrides whatever indication is contained inside this packet.
- **MS-MPPE-Recv-Key**: As defined by RFC 3078.
- **MS-MPPE-Send-Key**: As defined by RFC 3078.
- **Session-Timeout** (32-bit unsigned integer): Maximum time a session can be active. After this interval, the 802.1x client is re-authenticated.
- **Termination-Action**: As defined by RFC 2865. If set to 1, customer traffic is not allowed during the 802.1x re-authentication.
- **Tunnel-Medium-Type**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to 802.
- **Tunnel-Private-Group-ID**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to the VLAN ID.
- **Tunnel-Type**: Used only when assigning a specific VLAN number to a customer. In this case it must be set to VLAN.

9.1.2.3.2 Access Reject

Access Reject RADIUS attributes are not supported.

9.1.2.4 Access Challenge Attributes

This table lists all attributes supported in Access Challenge packets for each authentication type.

Attribute	Admin login	802.1X	MAC
EAP-Message		■	
Message-Authenticator		■	
State		■	

9.1.2.4.1 Descriptions

- **EAP-Message** (string): As defined in RFC 2869.
- **Message-Authenticator** (string): As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.

- **State** (string): As defined in RFC 2865.

9.1.2.5 Accounting Request Attributes

This table lists all attributes supported in Accounting Request packets for each authentication type.

Attribute	Web Admin	802.1X	MAC
Acct-Session-Id		■	■
Acct-Session-Time		■	
Acct-Status-Type		■	■
Called-Station-Id		■	■
Calling-Station-Id		■	■
Class		■	■
Framed-MTU		■	
NAS-Identifier		■	■
NAS-Port		■	■
NAS-Port-Type		■	■
User-Name		■	■
Alvarion-AVPair (SSID)			■

9.1.2.5.1 Descriptions

- **Acct-Session-Id** (32-bit unsigned integer): Random value generated by the AP.
- **Acct-Session-Time** (32-bit unsigned integer): Number of seconds this session since this session was authenticated.
- **Acct-Status-Type** (32-bit unsigned integer): Supported values are Accounting-On (7) and Accounting-Off (8).
- **Called-Station-Id** (string): BSSID of the wireless client, or the MAC address of the LAN port used by a wired client. By default, the MAC address is sent in IEEE format. For example: 00-02-03-5E-32-1A. This can be changed on the **Security > 802.1x** page.
- **Calling-Station-Id** (string): The MAC address of the 802.1x client station in IEEE format. By default, the MAC address is sent in IEEE format. For

example: 00-02-03-5E-32-1A. This can be changed on the **Security > 802.1x** page.

- **Class** (string): As defined in RFC 2865. Multiple instances are supported.
- **Framed-MTU** (32-bit unsigned integer): Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the profile being used.
- **NAS-Port** (32-bit unsigned integer): Always 0.
- **NAS-Port-Type** (32-bit unsigned integer): Always set to 19, which represents WIRELESS_802_11.
- **User-Name** (string): The RADIUS username provided by the 802.1x client.
- **Alvarion-AVPair** (SSID): SSID that the customer is associated with.

9.1.2.6 Accounting Response

Accounting Response RADIUS attributes are not supported.

9.1.3 Configuring Administrator Profiles on the RADIUS Server

To support more than one administrator username and password, you must use a RADIUS server to manage them. The AP itself supports a single administrator name and password internally.

CAUTION



Improper configuration of the administrator profile could expose the AP to access by any user with a valid account. The only thing that distinguishes an administrative account from that of a standard user account is the setting of the service type. Make sure that a user is not granted access if the service type is not Administrative.

This section presents all supported RADIUS and Alvarion attributes that can be used to configure an administrator profile on a RADIUS server. Attributes starting with *MS* are Microsoft and are not standard.

NOTE

In the following definitions strings are defined as 1 to 253 characters long.

NOTE

Only Access Request packets are supported. Access Accept, Access Reject, Access Challenge, Accounting Request, or Accounting Response requests are not supported.

9.1.3.1 Access Request Attributes

The following are supported Access Request RADIUS attributes.

- **User-Name** (string): The username assigned to the user or a device when using MAC authentication.
- **NAS-Identifier** (string): The NAS ID set on the **Security > RADIUS** page for the profile being used.
- **Service-Type** (32-bit unsigned integer): As defined in RFC 2865. Set as follows:
 - » Web Admin is SERVICE_TYPE_ADMINISTRATIVE
- **Framed-MTU** (32-bit unsigned integer): Hard-coded value of 1496.
- **MSCHAP-Challenge** (string): As defined in RFC 2433. Only present when the authentication scheme on the **Security > RADIUS** page is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.
- **MSCHAP-Response** (string): As defined in RFC 2433. Only present when the authentication scheme on the **Security > RADIUS** page is set to MSCHAPv1. Length = 49 bytes.

9.2 Managing Certificates

Digital certificates are electronic documents that are used to validate the end parties or entities involved in data transfer. These certificates are normally associated with X.509 public key certificates and are used to bind a public key to a recognized party for a specific time period.

Various features on the AP make use of X.509 certificates for authentication and/or encryption of data exchanged with peers.

The certificate stores provide a repository for managing all certificates. To view the certificate stores, select **Security > Certificate stores**.

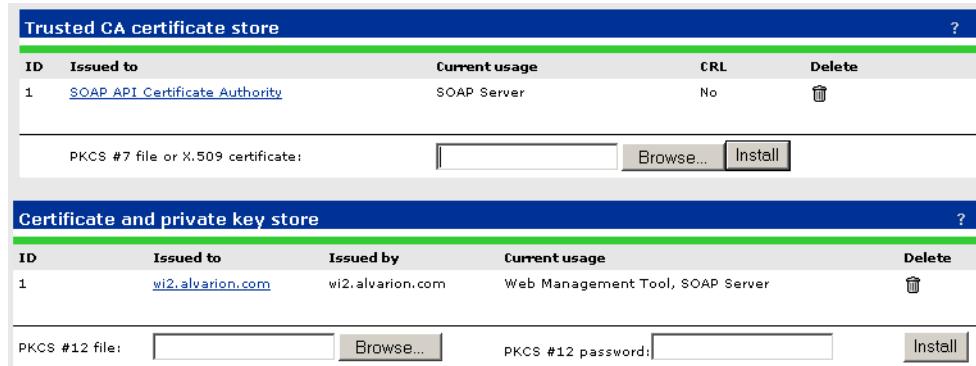


Figure 9-3: Managing Certificates

9.2.1 Trusted CA Certificate Store

This list displays all CA certificates installed on the AP. The AP uses the CA certificates to validate the certificates supplied by peers during authentication. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

The AP uses the CA certificates to validate certificates supplied by:

- Administrators accessing the AP's management tool
- SOAP clients communicating with the AP's SOAP server

The following information is displayed for each certificate in the list:

9.2.1.1 Issued to

Name of the certificate holder. Click the name to view the contents of the certificate.

9.2.1.2 Current Usage

Lists the services that are currently using this certificate.

9.2.1.3 CRL

Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.

9.2.1.4 Delete

Select to remove the certificate from the certificate store.

9.2.2 Installing a New CA Certificate

- 1 Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
- 2 Select **Install** to install a new CA certificate.

9.2.3 CA certificate Import Formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)
- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.

Content and file format	Items carried in the file	Description
X.509 certificate in PEM file	One or more X.509 certificate	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

9.2.4 Default CA Certificates

The following certificates are installed by default:

- **SOAP API Certificate Authority:** Before allowing a SOAP client to connect the AP checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).

NOTE



For security reasons, you should replace the default certificate with your own.

9.2.4.1 Certificate and Private Key Store

This list displays all certificates installed on the AP. The AP uses these certificates and private keys to authenticate itself to peers.

The following information is displayed for each certificate in the list:

9.2.4.1.1 Issued to

Name of the certificate holder. Select the name to view the contents of the certificate.

9.2.4.1.2 Issued by

Name of the CA that issued the certificate.

9.2.4.1.3 Current Usage

Lists the services that are currently using this certificate.

9.2.4.1.4 Delete

Select to remove the certificate from the certificate store.

9.2.4.2 Installing a New Private Key/public Key Certificate Chain Pair

NOTE



RADIUS EAP certificates must have the X.509 extensions. Information about this is available in the Microsoft knowledgebase at:
<http://support.microsoft.com/kb/814394/en-us>

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The name in the certificate is automatically assigned as the domain name of the AP.

- 1 Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
- 2 Specify the **PKCS #12 password**.
- 3 Select **Install** to install the certificate.

9.2.4.3 Default Installed Private Key/public Key Certificate Chains

The following private key/public key certificate chains are installed by default:

- **wireless.alvarion.com:** Default certificate used by the management tool and SOAP server.

NOTE

When a web browser connects to the AP using SSL, the AP sends only its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the web browser does not get the whole certificate chain it needs to validate the identity of the AP. Consequently, the web browser issues security warnings. To avoid this problem, install an SSL certificate on the AP only if it is directly signed by the root certificate authority or if you have appended all certificates that make up the chain.

Consequently, the web browser issues security warnings.

To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the AP.

NOTE

An SNMP trap is sent to let you know when the AP's SSL certificate is about to expire if you enable the **Traps** option on the **Management > SNMP** page and then click **Configure traps** and enable the **Certificate about to expire trap** option under **Maintenance**.

9.2.5 Certificate Usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:

Services using certificates		
Service	Authenticate to peer using	Number of associated CAs
Web Management Tool	1 - wi2.alvarion.com	0
SOAP Server	1 - wi2.alvarion.com	1

Figure 9-4: Certificate Usage

9.2.5.1 Service

Name of the service that is using the certificate. To view detailed information on the certificate select the service name.

9.2.5.2 Authenticate to Peer Using

Name of the certificate and private key. The AP is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the AP as a legitimate user of the certificate.

9.2.5.3 Number of Associated CAs

Number of CA certificates used by the service.

9.2.5.4 Changing the Certificate Assigned to a Service

Select the service name to open the Certificate details page. For example, if you select **Web management tool**, you will see:

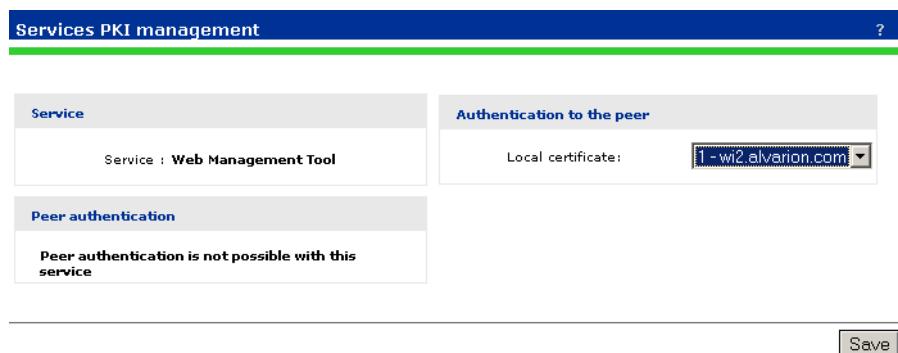


Figure 9-5: Changing the Certificate Assigned to a Service

Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

9.2.6 About Certificate Warnings

Access to the management tool must occur through a secure connection (SSL). Until a certificate is installed, certificate warnings will appear at login.

To continue to work with the management tool without installing a certificate, proceed as follows: At the security certificate prompt, in Microsoft Internet Explorer 7, select **Continue to this website**; in Firefox 2, select **Accept this certificate temporarily for this session** and **OK**.

To eliminate these warnings you can purchase a valid SSL certificate (from a source such as Verisign) that will work with the default configuration of your web browser, and install it on the service controller.

The following is an example of a security warning displayed by Internet Explorer 7:

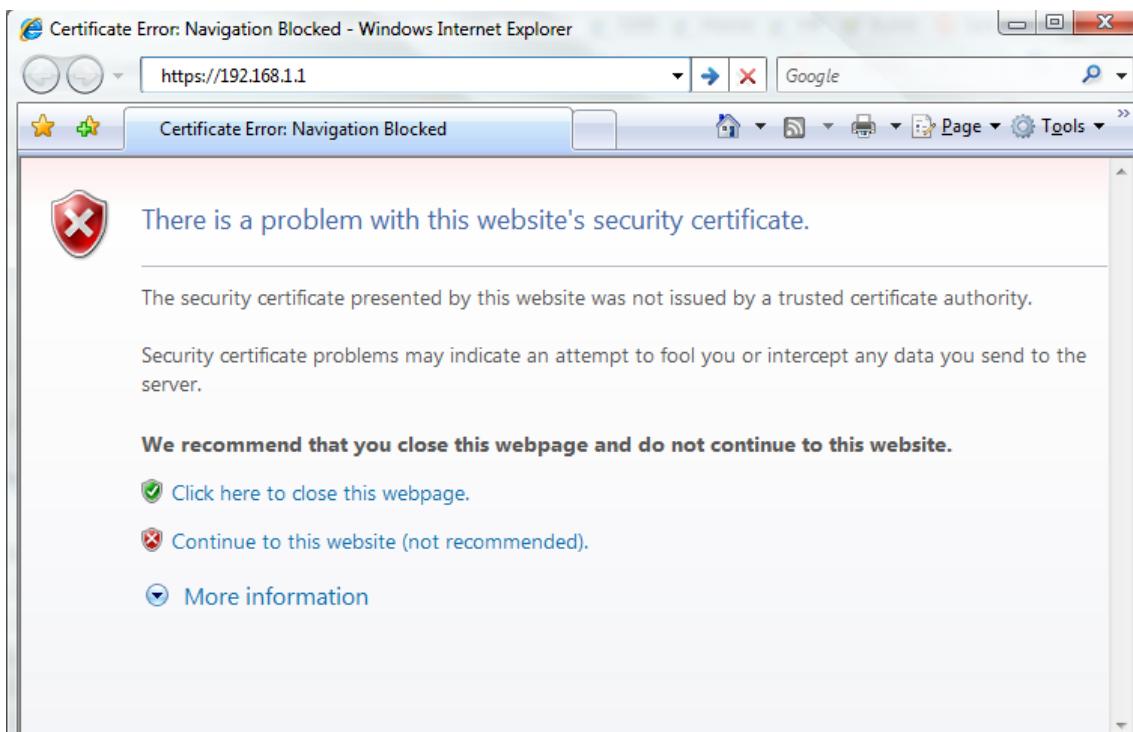


Figure 9-6: Certificate Warnings

Chapter 10 - Local Mesh

In This Chapter:

- “Key Concepts” on page 164
- “Local Mesh Terminology” on page 165
- “Local Mesh Profiles” on page 169
- “Configuration Considerations” on page 178
- “Quality of Service” on page 179
- “Configuration Summary” on page 180
- “How to Configure Local Mesh in Controlled Mode” on page 181
- “Sample Local Mesh Deployments” on page 195

10.1 Key Concepts

10.1.1 New in this Release

In previous releases, the *local mesh* feature was known as *DWDS* (dynamic wireless distribution system).

10.1.2 Benefits

The local mesh feature replaces the need for Ethernet cabling between APs, enabling expanded Wi-Fi coverage through the use of wireless bridges to transport network traffic in hard-to-wire or outdoor areas.

Key local mesh features include:

- **Automatic link establishment:** Nodes automatically establish wireless links to create a full-connected network. A dynamic network identifier (local mesh ID) restricts connectivity to local mesh nodes, enabling distinct local meshes to be created with nodes in the same physical area.
- **Provides fall-back operation to recover from node failure.** In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.

10.2 Local Mesh Terminology

10.2.1 Static Local Mesh Links

The following illustration and table define terms that are used in this guide when discussing the static local mesh feature.



Figure 10-1: Static Local Mesh Links

Term	Definition
Local	The AP that you are currently configuring to support a static link.
Remote	The AP that to which the static link will connect.
Link	The wireless connection between a local and remote AP.

10.2.2 Dynamic Local Mesh Links

The following illustration and table define terms that are used in this guide when discussing the dynamic local mesh feature.

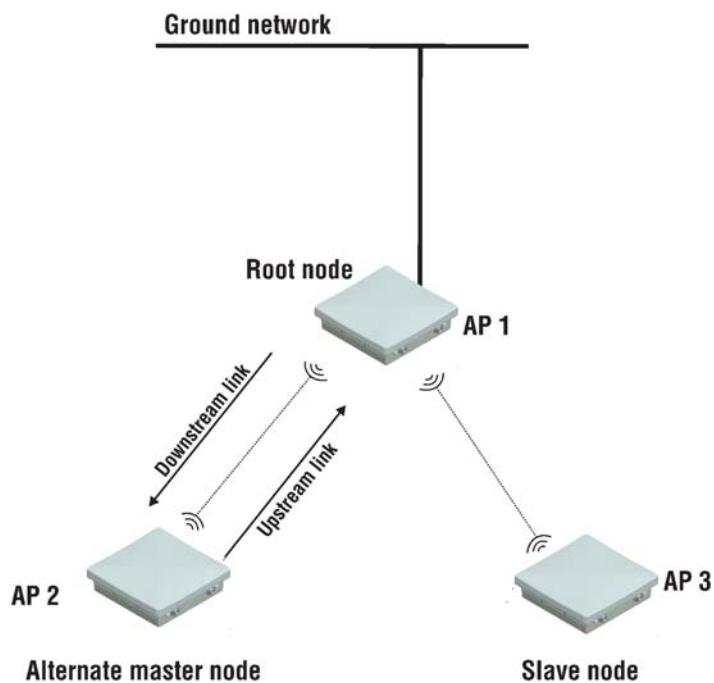


Figure 10-2: Dynamic Local Mesh Links

Term	Definition
Node	A AP that is configured to support local mesh connections.
Root node	The root node is configured in Master mode and provides access to the ground network.
Alternate master node	A node that is configured in Alternate master mode which enables it to make upstream and downstream connections.
Slave node	A node that is configured in Slave mode which enables it to make upstream connections only.
Ground network	Wired network to which the root node is connected. This is the network to which the local mesh provides access for all connected alternate master and slave nodes.
Mesh	A series of nodes that connect to form a network. Each mesh is identified by a unique mesh ID.
Link	The wireless connection between two nodes.
Downstream link	A link that transports data away from the ground network.
Upstream link	A link that transports data towards the ground network.
Peer	Any two connected nodes are peers. In the diagram, AP 1 is <i>the peer of both AP 2 and AP 3</i> .

10.2.2.1 Operational Modes

Three different roles can be assigned to a local mesh node: **Master**, **Alternate**

Master, or **Slave**. Each role governs how AP upstream and downstream links are established by the node.

- **Master:** Root node that provides the upstream link to the *ground network* that the other nodes want to reach. The master never tries to connect to any other node. It waits for links from downstream alternate master or slave nodes.

NOTE



It is possible to have several masters for the same mesh ID connected to the ground network. This can be used to provide redundant paths to the ground network for downstream nodes.

- **Alternate Master:** First establishes an upstream link with a master or alternate master node. Next, operates as a master node waits for links from downstream alternate master or slave nodes.
- **Slave:** Can only establish an upstream link with master or alternate master node. Slave nodes cannot establish downstream links with other nodes.

10.2.2.2 Node Discovery

Discovery of another node to link with is limited to nodes with the same mesh ID. The link is established with the node that has the best score based on the following calculation:

$$\text{Score} = \text{SNR} - (\text{Number of hops} \times \text{SNR cost of each hop})$$

If a node loses its upstream link, it automatically discovers and connects to another available node.

10.2.2.3 Operating Channel

If a mesh operates on a dynamic frequency selection (DFS) channel, the master node selects the operating channel. If another node detects radar and switches channels, that node reports the channel switch to the master node, which initiates a channel switch for the nodes connected to it. This allows the local mesh to converge on a specific channel.

A node that uses a DFS channel and that loses connection with its master, scans channels to find a master on another channel, which can be a new master or the same master.

If the local mesh does not operate on a DFS channel, configure the radios in one of the following ways:

- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master's channel and link with the master.

10.3 Local Mesh Profiles

A local mesh profile defines the characteristics for the type of links that can be established with other nodes. Each node supports up to six profiles, each of which can be either static or dynamic.

- If a profile defines a static local mesh link, the profile can only be used to connect with another node with a matching profile that has matching settings.
- If a profile defines a dynamic local mesh link, it establishes links to other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes.
Alternate master	A single link to a master node or alternate master node.	Up to eight links with alternate master or slave nodes.
Slave	A single link to a master node or alternate master node.	None.

When a dynamic profile is active, the AP constantly scans and tries to establish links as defined by the profile.

To view or add profiles select **Wireless > Local mesh**.

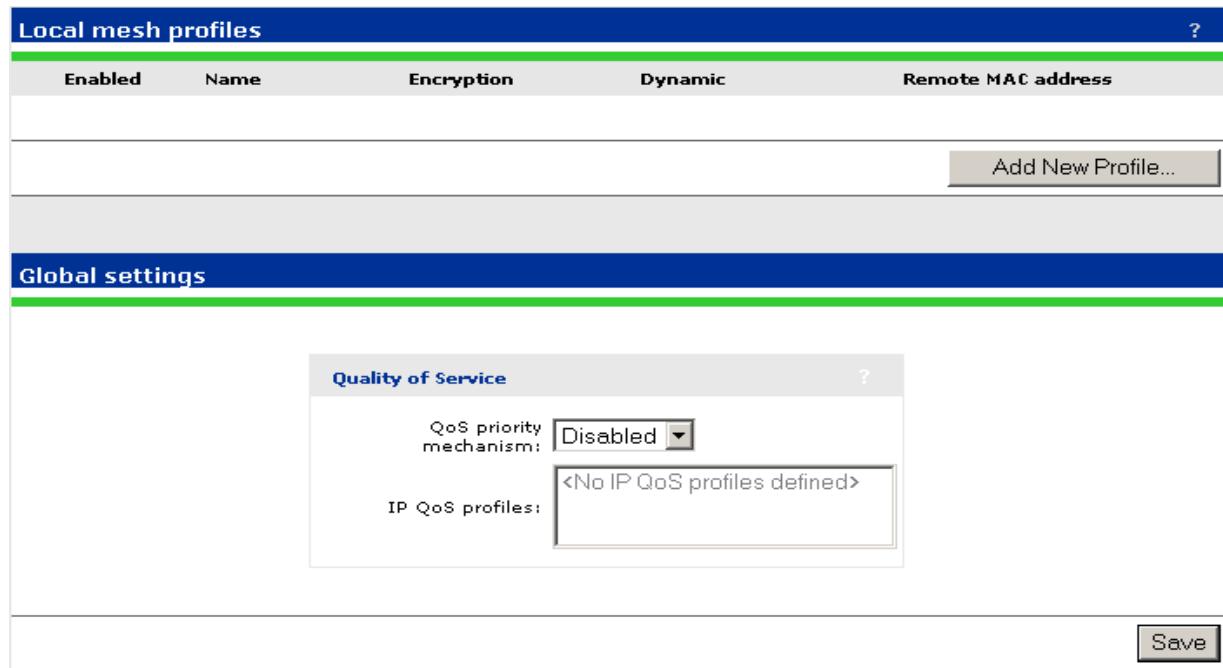


Figure 10-3: Local Mesh Profiles

To configure a profile, select its name in the list. Or to add a profile, select **Add New Profile**.

10.3.1 Configuring a Local Mesh Profile

To configure a profile, click its name in the list. The **Local mesh profile** page opens.

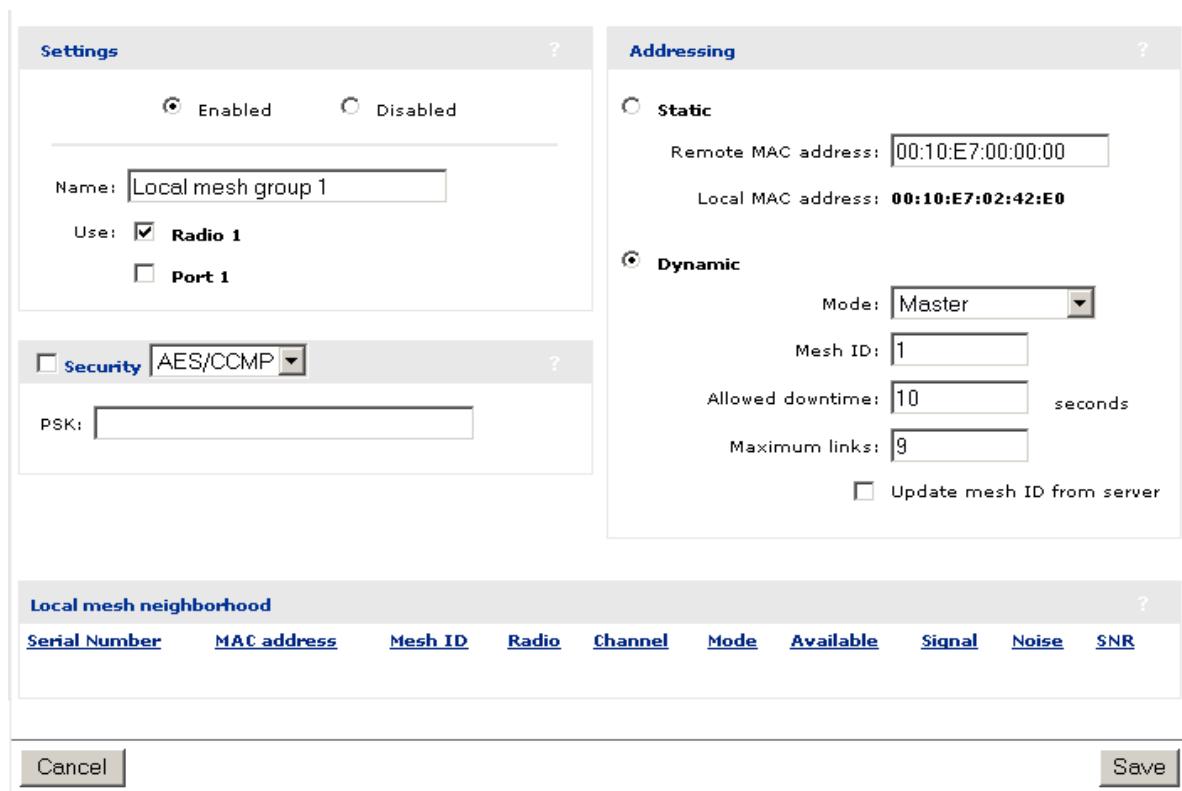


Figure 10-4: Configuring a Local Mesh Profile

10.3.1.1 Settings

10.3.1.1.1 Enabled/Disabled

Specify if the profile is enabled or disabled. The profile is only active when enabled.

10.3.1.1.2 Name

Name of the profile.

10.3.1.1.3 Use

Select the interface to use for this link.

10.3.1.1.4 Speed

(Static links only)

Sets the speed the link will operate at. For load balancing you may want to limit the speed of a link when connecting to multiple destinations.

10.3.1.2 Security

Enable this option to secure data transmitted on the wireless link. The APs on both sides of the wireless link must be configured with the same security options.

10.3.1.2.1 WEP

Enables WEP to secure traffic on the wireless link.

Specify the encryption key the node will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

10.3.1.2.2 TKIP

Enables TKIP encryption to secure traffic on the link.

The node uses the key you specify in the PSK field to generate the TKIP keys that encrypt the wireless data stream.

Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long, and be a mix of letters and numbers.

10.3.1.2.3 AES/CCMP

Enables AES with CCMP encryption to secure traffic on the link. This is the most secure method.

The node uses the key you specify in the PSK field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

10.3.1.3 Addressing

10.3.1.3.1 Static

Use this option to create simple back-to-back links between two APs. When creating static links, both APs must be operating on the same wireless channel. Make sure that the channel selection on the **Wireless > Radio(s)** page is not set to **Automatic**.

10.3.1.3.2 Remote MAC Address

MAC address of the radio on the remote AP on which the link will be established.

Local MAC address

MAC address of the radio on this AP on which the link will be established.

10.3.1.3.3 Dynamic

Use this option to create dynamic local mesh installations.

10.3.1.3.3.1 Mode

Three different roles can be assigned to a node: master, alternate master, or slave. The role assigned to a node, governs how the node will establish upstream or downstream links with its peers. The available configuration settings change depending on the role that is selected.

- » **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream links to alternate master or slave nodes.

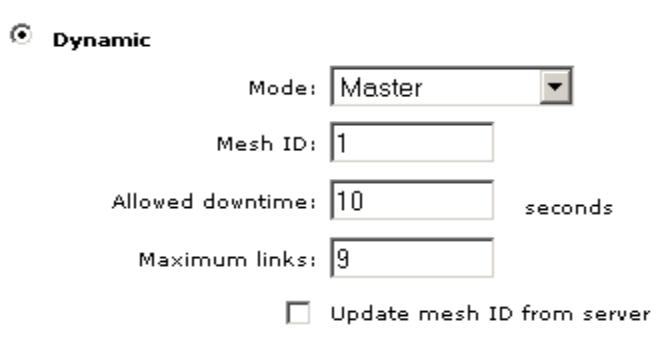


Figure 10-5: Dynamic: Master Mode

- » **Slave:** Slave nodes can only establish upstream links with master or alternate master nodes. Slave nodes cannot establish downstream links with any other nodes.

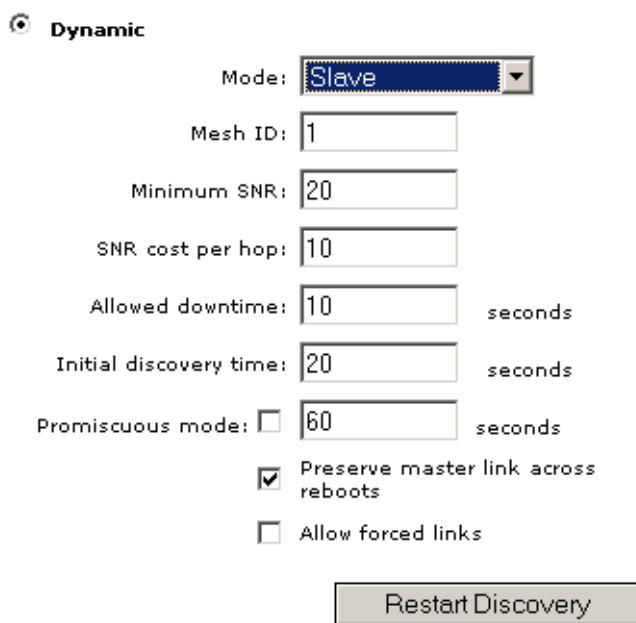


Figure 10-6: Dynamic: Slave Mode

- » **Alternate Master:** An alternate master node must first establish an upstream link with a master or alternate master node before it can establish downstream link with an alternate master or slave node.

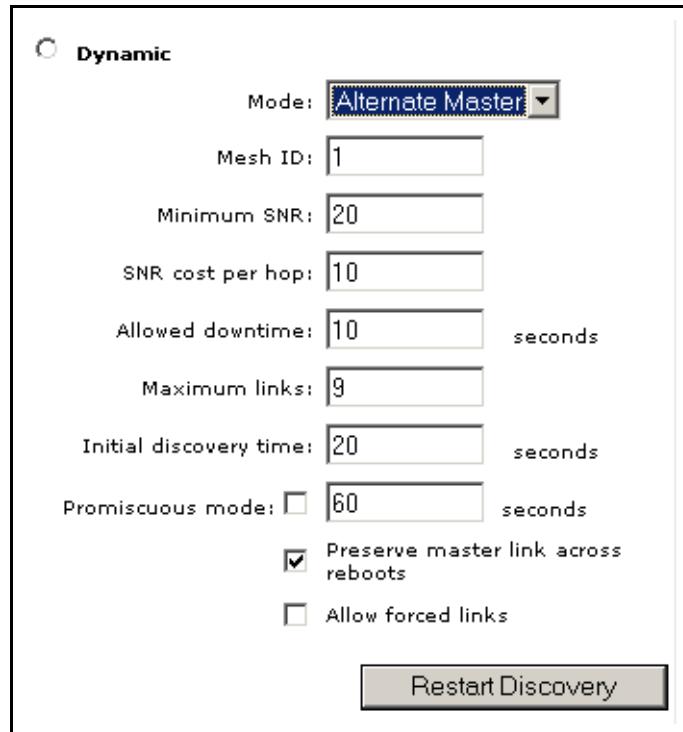


Figure 10-7: Dynamic: Alternate Master Mode

10.3.1.3.3.2 Mesh ID

Unique number that identifies a series of nodes that can connect together to form a local mesh network.

10.3.1.3.3.3 Minimum SNR

(Alternate master or slave nodes)

This node will only connect with other nodes whose SNR is above this setting (in dB).

10.3.1.3.3.4 SNR Cost Per Hop

(Alternate master or slave nodes)

This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.

10.3.1.3.3.5 Allowed Downtime

The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate master) loses its link to its master, the discovery phase is re-initiated.

10.3.1.3.3.6 Maximum Links

(Master or alternate master nodes only)

The maximum number of upstream and downstream links that this node can support.

10.3.1.3.3.7 Initial Discovery Time

(Alternate master or slave nodes)

Amount of time that will be taken to discover the best available master node. The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

10.3.1.3.3.8 Maximum Links

The maximum number of upstream and downstream links that this node can support.

10.3.1.3.3.9 Promiscuous Mode

(Alternate master or slave nodes)

Although it could be used in other applications, the promiscuous mode is primarily intended to solve issues specific to local mesh networks aboard trains. The main issue that it addresses is train configuration changes. When a car is taken out for maintenance and replaced with a new one, the AP in that new car will not be able to connect to the train's local mesh network because it is configured with a different mesh ID. This is where the promiscuous mode comes into play. Its goal is to allow a node to connect to a different mesh when it could not find any available master (alt-master) in its mesh for a certain, configurable, amount of time.

When a node joins a new mesh, it is considered to be the consequence of a car change (or replacement of an AP). This event triggers the following actions:

- » The node's firmware is updated, given that a firmware update URL is configured.
- » The node's configuration is updated, given that a configuration file URL is configured. This will consequently change the node's mesh ID to the one found in the configuration file. If no configuration file URL is provided, the node will immediately proceed with updating its mesh ID.
- » An SNMP trap is sent.

NOTE

After completing a configuration or firmware download, a local mesh node will wait an additional 30 seconds before rebooting if a downstream link was established with another node in promiscuous mode. The purpose of this delay is to give downstream nodes some more time to download their firmware and configuration, improving the total convergence time of an entire train network after a master car change.

[10.3.1.3.3.10 Preserve Master Link Across Reboots](#)

(Alternate master or slave nodes)

When this option is enabled, the AP will first try re-connecting to the master (alt-master) it was connected to before rebooting (or disabling/re-enabling the profile). This re-connection happens during the initial discovery time. After that period, the regular best master identification mechanism will take over.

[10.3.1.3.3.11 Allow Forced Links](#)

(Alternate master or slave nodes)

This option allows the AP to accept forced links from a master (alt-master). A link is forced from the master by using the force link button next to the slave's entry in the local mesh scan. A link can be forced to a slave (alt-master) in a different mesh. This will cause the slave to save the new mesh ID and use it from that point onward.

[10.3.1.3.3.12 Update Mesh ID from Server](#)

(Master nodes only)

This is similar to promiscuous mode, but for a master. It is primarily used in train application. When this option is enabled, the master will check if the mesh ID in the configuration file on the server is the same as the mesh ID locally configured. The server (and configuration file name) is specified in the URL located in **Maintenance > Config file management > Scheduled operations**.

This allows a master AP to be replaced without changing the mesh ID of a train and without having to configure that AP to use this mesh ID. The mesh ID is stored on the server.

[10.3.1.3.3.13 Restart Discovery](#)

(Alternate master or slave nodes)

This button tells the AP to bring down any link it has already established and restart looking for the best master to which it can connect. It can be used when a new master is installed close to a slave and you want the slave to connect to that master, without rebooting.

10.4 Configuration Considerations

10.4.1 Simultaneous AP and Local Mesh

A radio can be configured to simultaneously support wireless clients and the creation of one or more local meshes. Although this offers flexibility it does have several limitations as follows:

- It reduces overall throughput since the total available bandwidth is shared between the local meshes and wireless users.
- It limits you to using the same radio options for both wireless clients and local meshes.

10.4.2 Maximum Range

The **Maximum range** setting on the **Wireless > Radio(s)** page can be used to fine tune internal timeout settings to account for the distance that a local mesh link spans. For normal operation, the timeout is optimized for links of less than 1 km.

NOTE



This is a global setting that applies to all wireless connections made with a radio, not just for local mesh links. Therefore, if you are also using a radio to serve local wireless users, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

10.5 Quality of Service

The local mesh feature enables you to define a quality of service (QoS) setting that will govern how traffic is sent on all wireless links.

The QoS setting on all nodes in a local mesh must be the same.

NOTE



When traffic is forwarded onto a local mesh link from a Virtual Network, the QoS settings on the Virtual Network take priority. For example, if you define a Virtual Network with a QoS setting of Virtual Network-based High, then traffic from this Virtual Network will traverse the bridge on queue 2 even if the QoS setting on the bridge is Virtual Network-based Low (queue 4).

10.6 Configuration Summary

- You can configure a total of six local mesh profiles on each node.
- Each dynamic local mesh profile (master or alternate master) can be used to establish up to nine links with other nodes.
- The same security settings must be used on all nodes in the same mesh.
- Daisy-chaining of nodes reduces throughput (which is typically divided by two for each hop) especially when one or more of the following are true:
 - » Nodes provide both upstream and downstream links on the same radio.
 - » Nodes share a radio with AP functionality.

10.7 How to Configure Local Mesh in Controlled Mode

The configuration of local mesh in controlled mode comprises the following steps:

- Setting a Master Profile
- Setting the Master AP
- Setting the SLAVE AP
- Adding the Slave AP in a Group on the Controller

10.7.1 Setting a Master Profile



To set a Master Profile:

Using a factory reset controller do the following:

- 1 Create a new Group within the controller by clicking on "**Controlled APs > Group Management > Add a new group**"

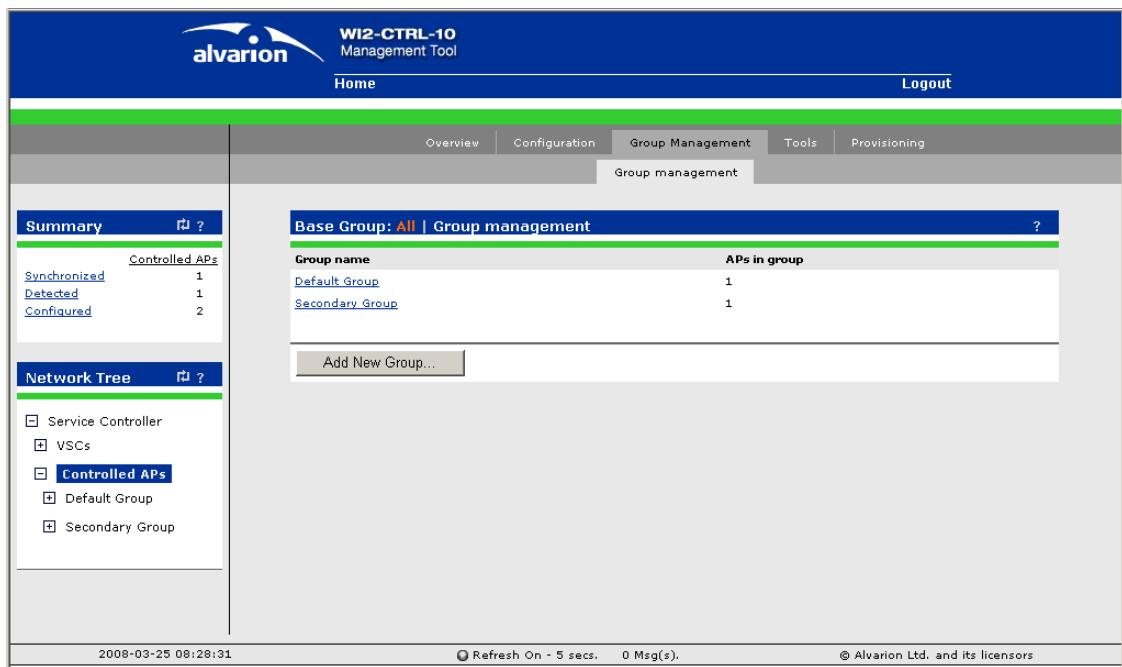
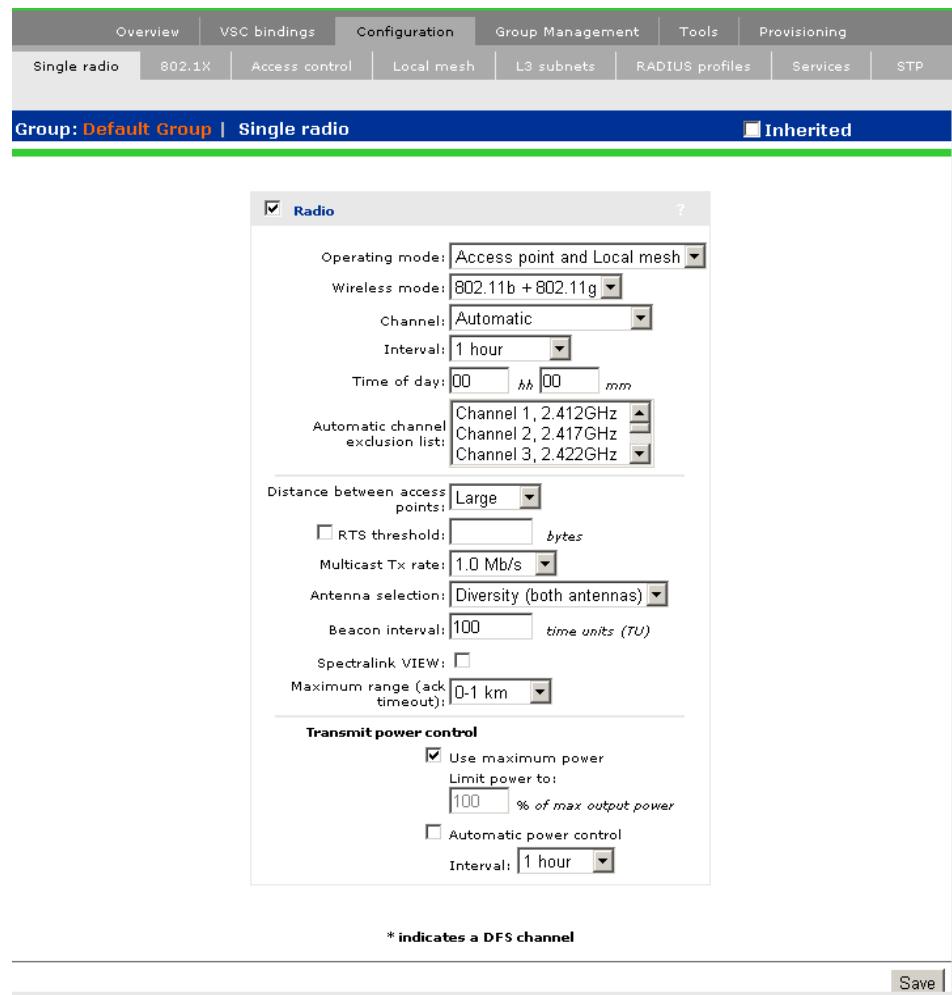


Figure 10-8: Group Management

- 2 Access the created group and click on the "Configuration" tab. The "Single Radio" page is displayed.
 - a Uncheck the "Inherited" check box
 - b Configure the Radio page as follows:

**Figure 10-9: Single Radio Page**

- c** Save your changes

- 3** Click on the "Local Mesh" tab located also under "Configuration"
 - a** Select "Local Mesh Profile # 1"
 - b** Uncheck the "Inherited" check box
 - c** Configure the profile as follows:

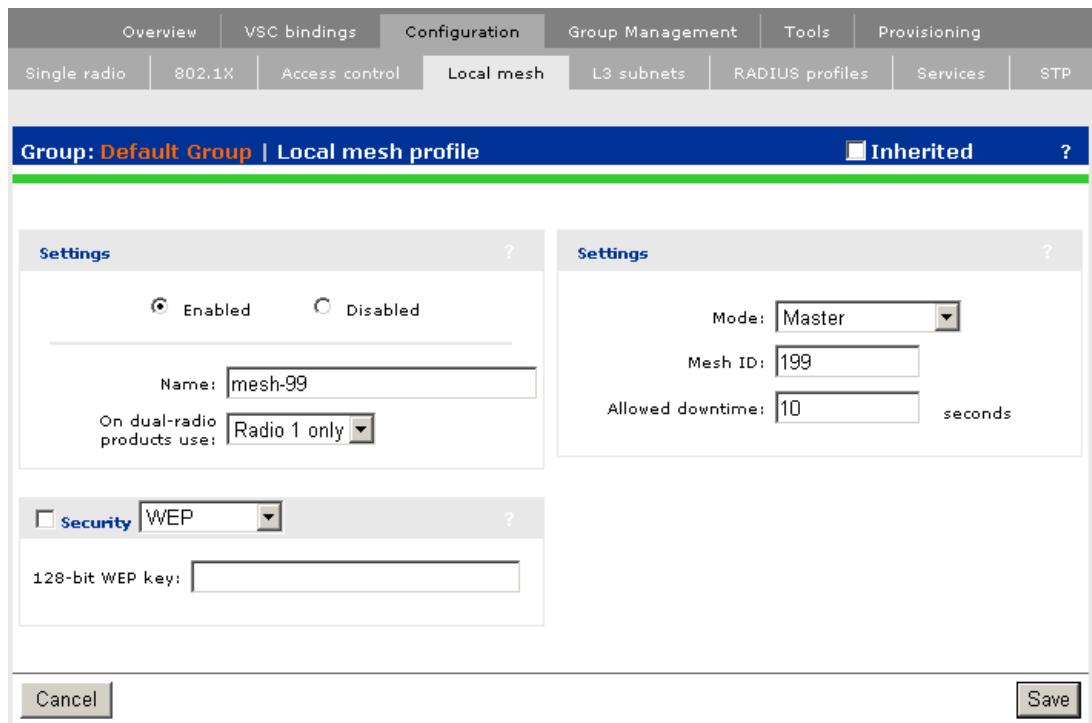


Figure 10-10: Local Mesh Profile

- d Save your configuration
- 4 Click on the "VSC" link in the Navigation tree bar
 - a Reconfigure the default VSC OR Click on the "Add a new VSC" Button, and configure a VSC as follows:

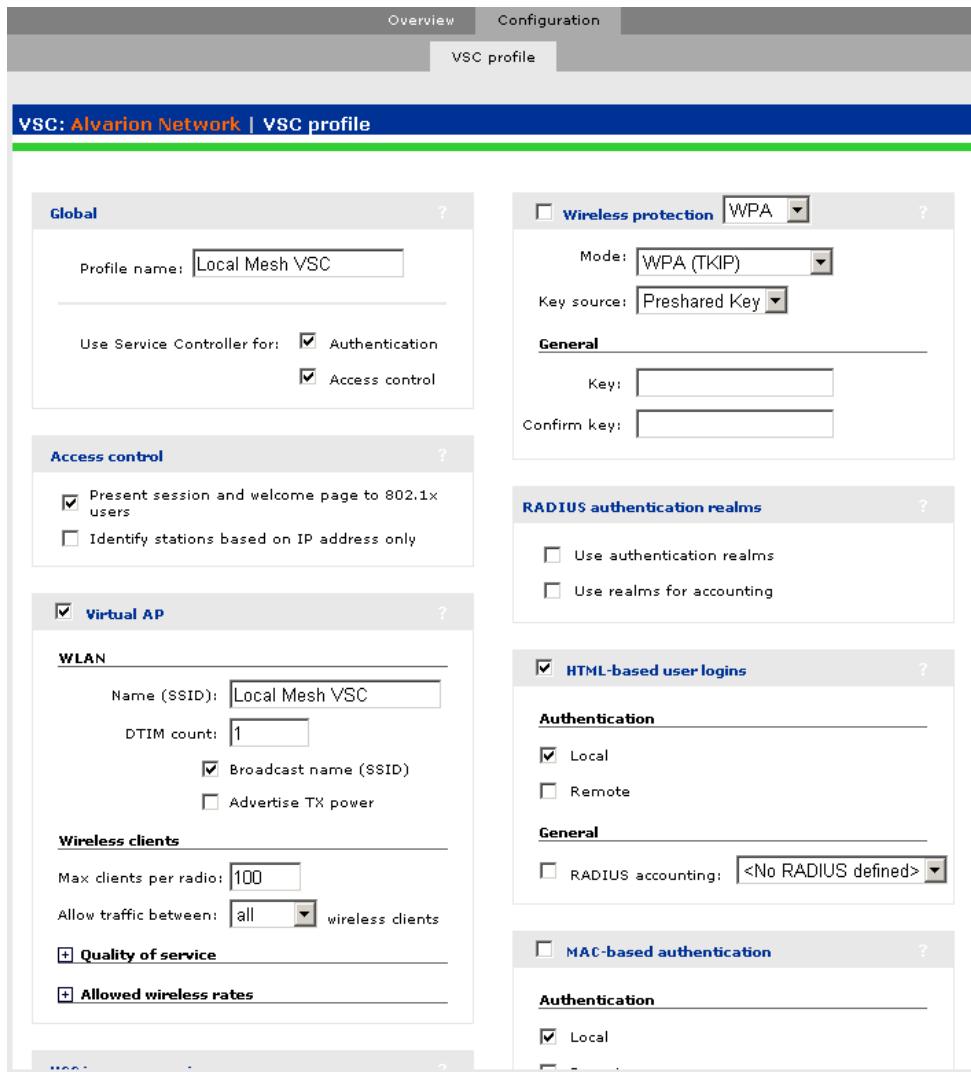


Figure 10-11: VSC Profile

- b** Save your configuration
- 5** Access the Group created in [Section 10.7.1](#) step1 above and click on the "VSC Bindings" tab.
 - a** Click on the "Add New Binding" button
 - b** Select the created VSC name in the "VSC Profile" menu as follows:

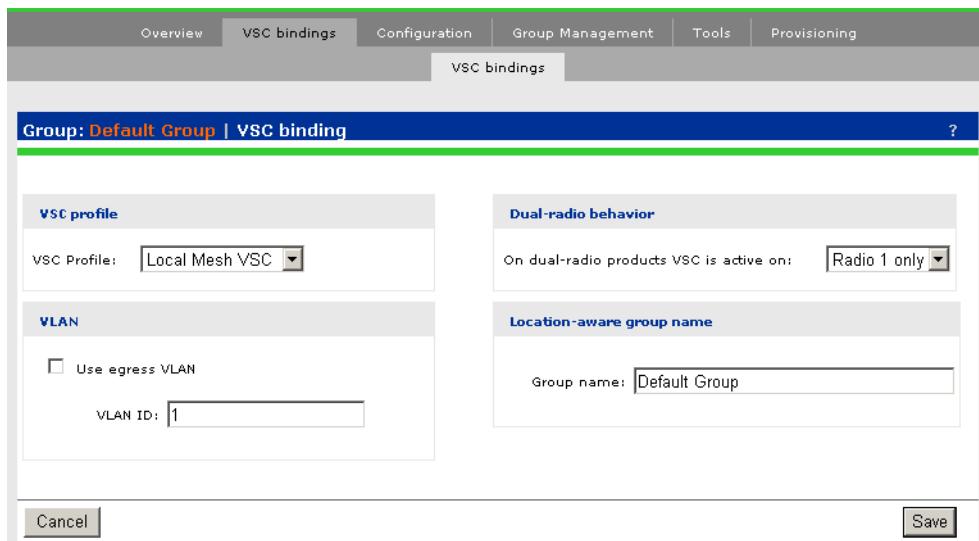


Figure 10-12: VSC Bindings

c Save your configuration

10.7.2 Setting the Master AP

- 1 Power UP an AP in Autonomous mode (Alvarion Default Mode)
- 2 Login to the AP's web tool
- 3 Click on "Maintenance > System"
- 4 Click on the "Switch to Controlled Mode" button to switch the MASTER AP into Controlled mode as shown below:

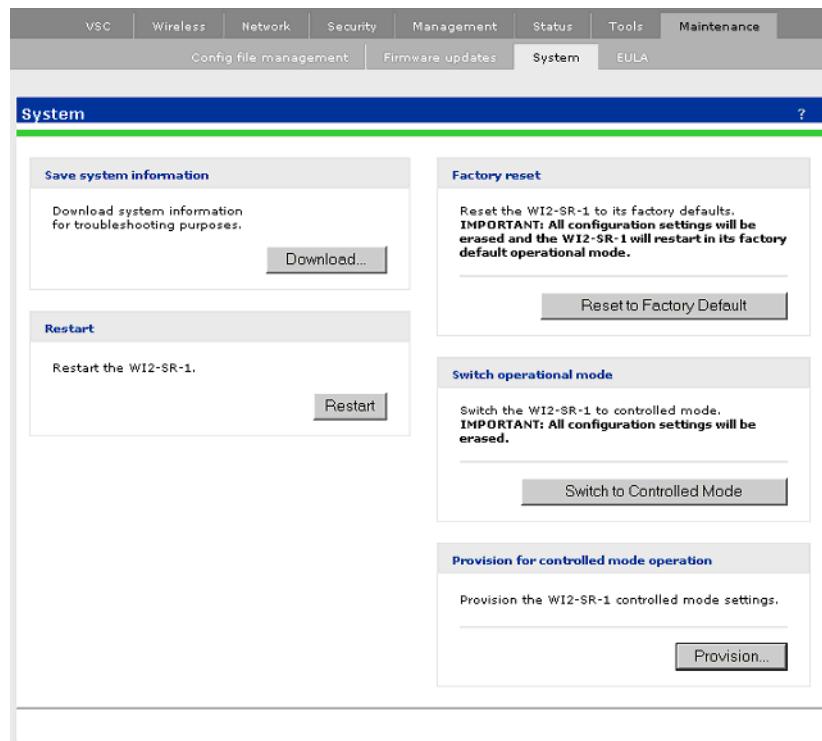


Figure 10-13: Switch to Controlled Mode

- 5 When this AP is back UP, place it on the same subnet as your controller
- 6 The AP should now discover the controller and synchs UP in the controller's DEFAULT GROUP
- 7 Drag and drop this AP from the DEFAULT GROUP into the created group in [Section 10.7.1 step1](#)
- 8 The AP should now synch into the created group restoring all the configuration done in STEPS (2 - 5)
- 9 Now you will have an active VSC bounded to the MASTER

10.7.3 Setting the SLAVE AP

- 1 Power UP another AP in Autonomous mode (Alvarion Default Mode)
- 2 Login to the AP's web tool
- 3 Click on "Maintenance > System"
- 4 Click on the "Provisioning" button at the bottom on this page to start provisioning the SLAVE AP

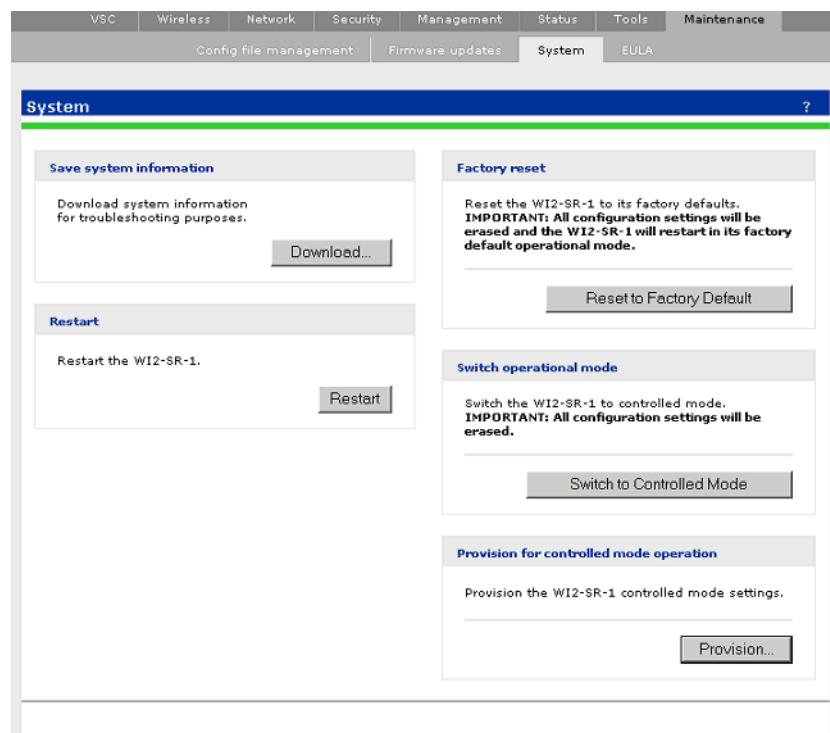


Figure 10-14: Provisioning the Slave AP

- 5 Starting with the "Connectivity" sub-page, configure as follows:

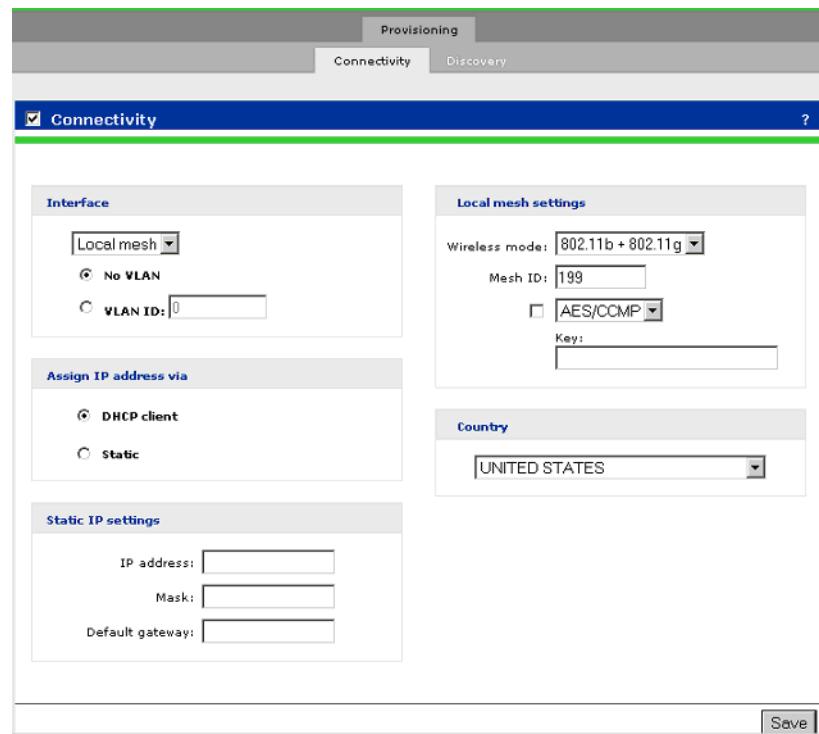


Figure 10-15: Connectivity Page

- 6 Save your configuration
- 7 Click on the Discovery sub-tab (within the provisioning page), and configure as follows:

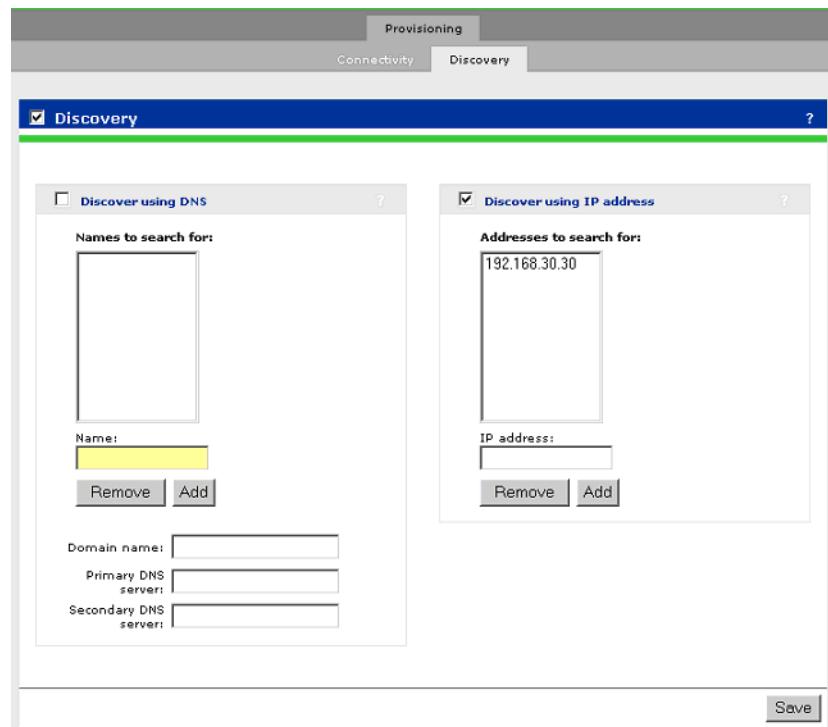


Figure 10-16: Discovery Page

NOTE

That the IP address showing in the "Discover using IP address" list should be your controller IP address

8 Save your Configuration.

9 Restart the AP by clicking on the restart button on this page.

10.7.4 Adding the Slave AP in a Group on the Controller

1 The provisioned SLAVE AP should discover the Controller over the Mesh Link. (Leave the SLAVE AP in the DEFAULT GROUP for now.)

NOTE

The Master and Slave APs can either share a group or be placed in different Groups. This section shows the different groups path for simplicity.

2 Create a new Group within the controller by clicking on "Controlled APs > Group Management > Add a new group" (see [Figure 10-8](#))

- 3 Access the created group and click on the "Configuration" tab. The "Single Radio" page is displayed.
 - a Uncheck the "Inherited" check box
 - b Configure the Radio page as in [Figure 10-9](#).
 - c Save your Configuration
- 4 Click on the "Local Mesh" tab located also under "Configuration"
 - a Select "Local Mesh Provisioning Profile"
 - b Configure as follows:

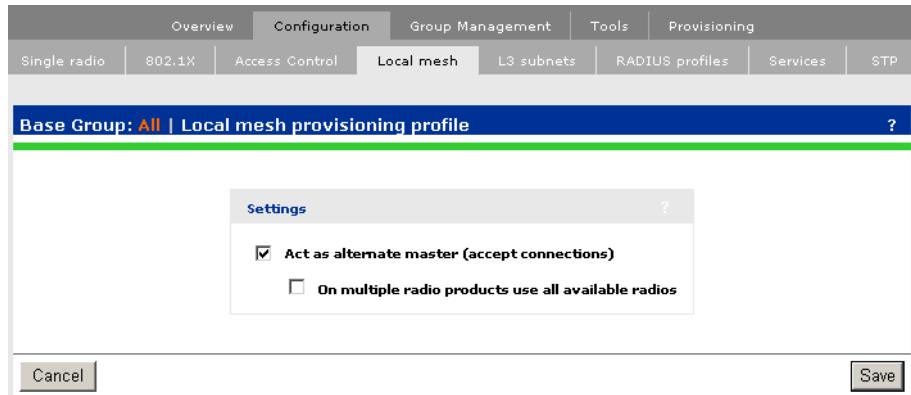


Figure 10-17: Local Mesh Provisioning Profile

- c Save your configuration.
- 5 Click on the "VSC" link in the Navigation tree bar
 - a Click on the "Add a new VSC" Button, and configure a VSC as follows (with a different SSID than the Masters):

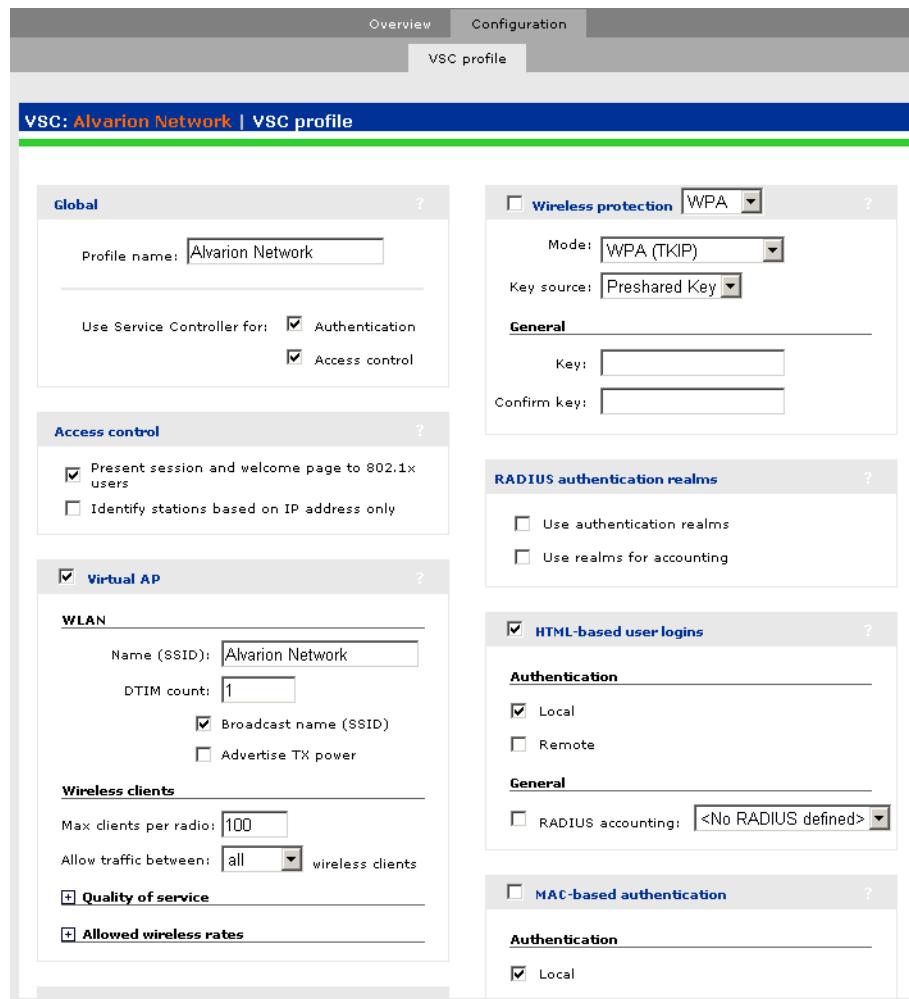
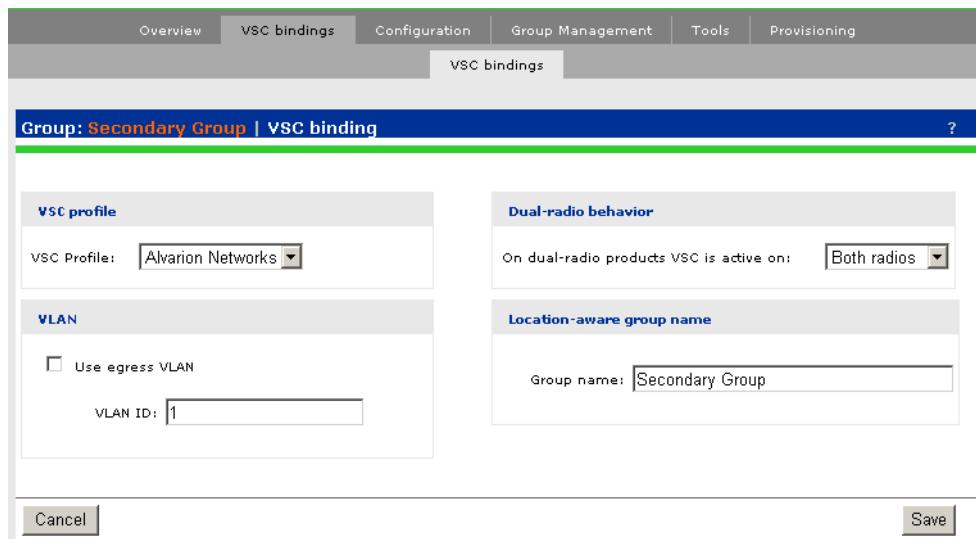


Figure 10-18: Adding a New VSC

- b** Save your configuration.

- 6** Access the Group created in [Section 10.7.4](#) step 2 above and click on the "VSC Bindings" tab.
 - a** Click on the "Add New Binding" button
 - b** Select the created SLAVE VSC name in the "VSC Profile" menu as follows:

**Figure 10-19: VSC Bindings - Slave**

- c** Save your configuration.
- 7** Drag and drop this AP from the DEFAULT GROUP into the created group in [Section 10.7.4](#) step 1.
- 8** The AP should now synch into the created group restoring all the configuration done in STEPS (3 - 5)
- 9** You now have an Active VSC on the SLAVE AP and a Local Mesh Link between the MASTER and the SLAVE.

10.7.5 Operation Verification



To verify that the link is UP:

- 1** Click on the "Controlled AP" link on the navigation tree of the Controller.
- 2** Click on "Local Mesh Link", you should see links that looks like the following:

The screenshot shows the management interface for a local mesh network. On the left, there's a sidebar with sections for Summary (Controlled APs: Synchronized 2, Detected 2, Configured 2) and Network Tree (Service Controller, VSCs, Local-Mesh-VSC, Sami-LM-Slave-Alv, Sami-Alv-Radius-VSC, Controlled APs, Default Group, Local-Mesh-Group, A733008507, local-Mesh-Group-NonMaster, A731034619). The main area has tabs for Overview, Configuration, Group Management, Tools, Provisioning, Local mesh neighborhood, Local mesh links (which is selected), and Licenses. The Local mesh links section displays a table of two links:

Type	From	To	Profile name	Mesh ID	Mode	Security	Link #
Slave link	A733008507	00:10:e7:02:40:80	mesh-199	199	Master	None	1
Master link	A731034619	00:10:e7:02:3f:d0	Local mesh provisioning profile	199	Slave	None	1

Figure 10-20: Link Verification

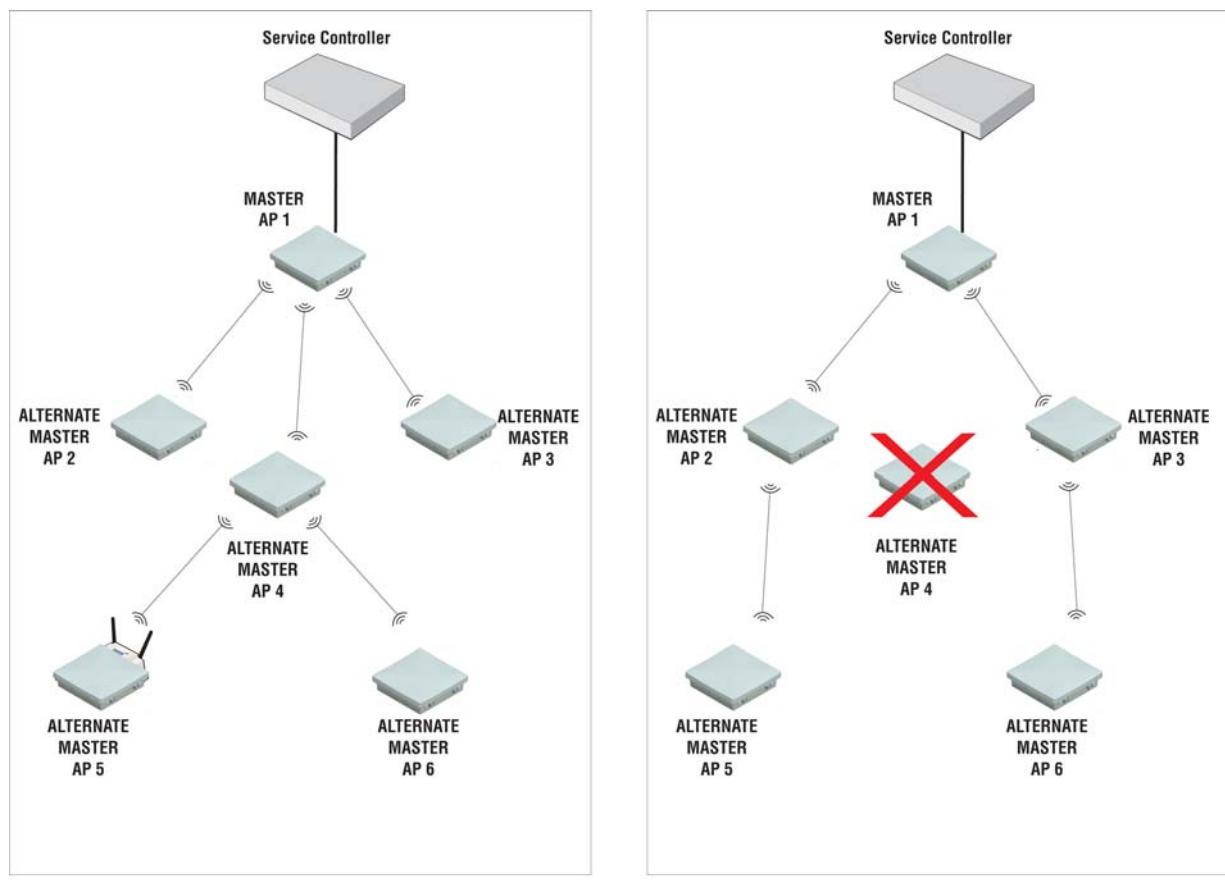
10.8 Sample Local Mesh Deployments

10.8.1 Dynamic Networks

In this scenario, a service controller is deployed with several APs to provide wireless coverage of a large area. Instead of using a backbone LAN, wireless links are used to interconnect all APs.

AP 1 is the *master*. It provides the connection to the wired network and a wireless link to the other APs. The other APs automatically established their links to the master based on a balance between SNR (signal to noise ratio) and hops, to provide the most efficient network topology.

If a node becomes unavailable, the links dynamically adjust to find the optimum path to the master.



Initial network configuration is automatically established.

When AP 4 is unavailable, the network dynamically reconfigures itself.

Figure 10-21: Dynamic Networks

Chapter 11 - Maintenance

In This Chapter:

- “Config File Management” on page 198
- “Firmware Updates” on page 204
- “Licenses” on page 207

11.1 Config File Management

The configuration file contains all the settings that customize the operation of the AP. You can save and restore the configuration file manually, automatically, or with a tool like cURL.

Select **Maintenance > Config file management**.

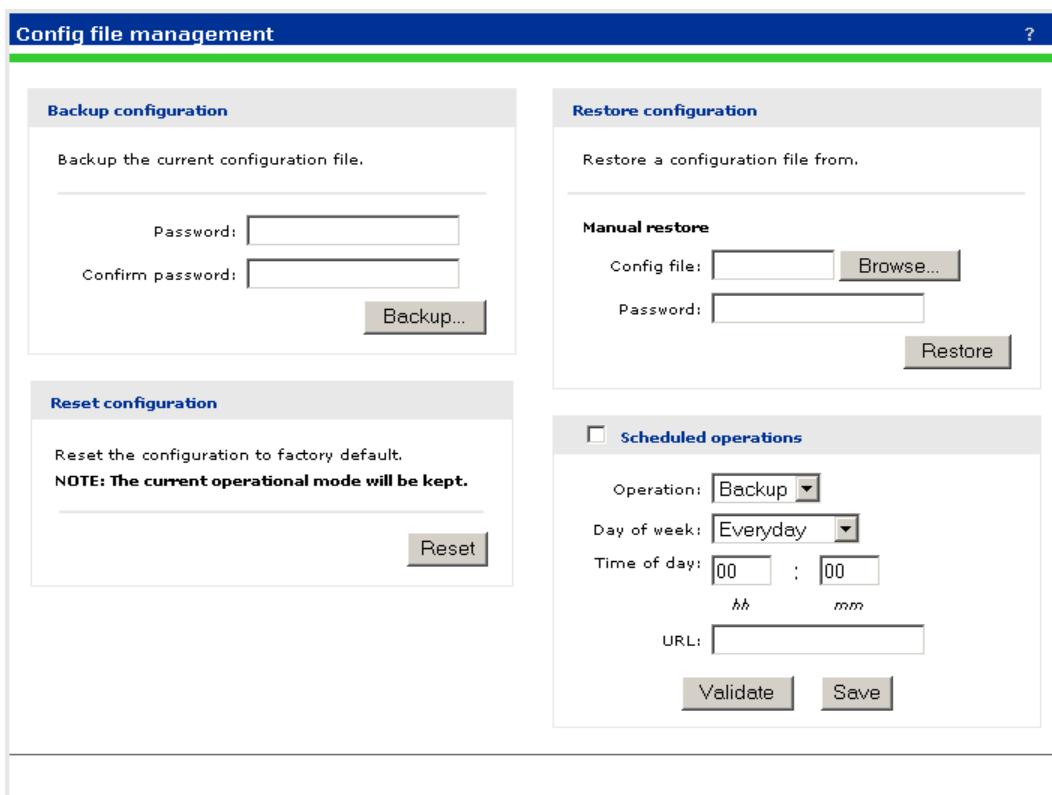


Figure 11-1: Config File Management

11.1.1 Manual Configuration File Management

The following options are available for manual configuration file management.

11.1.1.1 Backup Configuration

The **Backup configuration** group box enables you to back up your configuration settings so that they can be easily restored in case of failure. You can also use this option if you want to directly edit the configuration file.

Before you install new firmware, you should always back up your current configuration. Select **Backup** to start the process. You are prompted for the location in which to save the configuration file.

If you specify a **Password**, the configuration file is protected by encrypting sensitive fields (example, passwords, secrets, and certificates) with a key based on the password. See also [Restore Configuration](#) below.

NOTE



Even without a password, the certificates are still encrypted but with a key that is identical on all devices.

NOTE



The local username and password for the administrator are not saved to the backup configuration file. If you upload a configuration file, the current username and password are not overwritten.

11.1.1.2 Reset Configuration

See “[Resetting to Factory Defaults](#)” on page 215.

11.1.1.3 Restore Configuration

The **Restore configuration** group box enables you to reload a previously saved backup configuration file.

This feature enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the AP or if you are managing several APs from a central site.

Use the following steps to restore a saved configuration file.

- 1 Select **Maintenance > Config file management**. The **Config file management** page opens.
- 2 In the **Restore configuration** group box under **Manual restore**, select **Browse** to navigate to and select the configuration file that you want to restore.
- 3 If the configuration file is protected with a password (see [Backup Configuration](#)) you must supply the correct password to restore the complete configuration. If you supply an invalid password, all settings are restored except the certificates.
- 4 To upload the selected file to the AP, select **Restore**.

NOTE

The AP automatically restarts when the upload is complete.

11.1.2 Scheduled Operations

The **Scheduled operations** group box enables you to schedule unattended backups or restorations of the AP's configuration file. See also “[Scheduled Update](#)” on page 205.

Use the following steps to schedule a backup or restoration of the AP's configuration file.

- 1 Select **Maintenance > Config file management**. The **Config file management** page opens.
- 2 At lower right, select the **Scheduled operations** checkbox.
- 3 Under **Operation**, select **Backup** or **Restore**.
- 4 Under **Day of week**, select **Everyday**, or select a specific day of the week on which to perform the backup or restoration.
- 5 Under **Time of day**, specify the hour and minute on which to perform the backup or restoration. Use the format *hh mm*, where
 - » *hh* ranges from 00 to 23
 - » *mm* ranges from 00 to 59
- 6 Under **URL**, specify the path that leads to the local or remote directory in which to save the configuration file or from which to load the configuration file. For example
 - » **ftp://username:password@192.168.132.11/new.cfg**
 - » **http://192.168.132.11/new.cfg**
- 7 To confirm that the specified **URL** is correct, select **Validate**.
- 8 To commit the schedule that you have configured, select **Save**.

11.1.3 Managing the Configuration File with cURL.

NOTE



This is an advanced topic. It is recommended that you perform configuration file management as described in the immediately-previous sections [Manual Configuration File Management](#) or [Scheduled Operations](#).

You can perform configuration-file-related tasks using the free tool cURL (<http://curl.haxx.se/>), version 7.1.0 or higher.

The following cURL commands shows you how to manage the configuration file. The following setup is assumed:

- IP address of the port 1 is 24.28.15.22.
- Management access to the port 1 is enabled.
- Configuration file is **new.cfg**.

These examples are not secure—that is, no certificates are used for authentication—but data traffic is encrypted.

NOTE



To secure the connection with the AP using certificates, use the --cacert option to specify where the CA certificates are located on your computer. You must also specify the host name **wireless.alvarion.com** instead of using an IP address. The host name must be resolved either by using a DNS server or using the hosts file on your computer.

NOTE



The first time an AP is started up after a factory reset, the end user license agreement must be accepted and the country of operation must be set. This must be done manually or be modifying the sample cURL scripts in this section.

11.1.3.1 Uploading the Configuration File

- 1 Prepare the AP to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

- 2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
-d pw=admin
```

- 3 Prepare the AP to receive the configuration update.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/config_init.asp"
```

4 Upload the configuration file.

```
curl -s -k --cookie cookie.txt -F config=@new.cfg -F backup=Restore  
"https://24.28.15.22/goform/ScriptUploadConfig"
```

5 Reset the AP to activate the new configuration.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/reset.asp"
```

11.1.3.2 Downloading the Configuration File

1 Prepare the AP to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d  
username=admin  
-d pw=admin
```

3 Prepare the configuration file for download.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/goform/FormBackupConfig"  
-d backup=Backup
```

4 Download the configuration file.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/download/new.cfg" -o new.cfg
```

5 Log out.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/goform/Logout" -d  
logout=Logout
```

11.1.3.3 Resetting the Configuration to Factory Defaults

See also “Resetting to Factory Defaults” on page 215.

1 Prepare the AP to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d  
username=admin  
-d pw=admin
```

3 Reset configuration to factory defaults.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/goform/  
ScriptResetFactory?reset=Reset+to+Factory+Default"
```

- 4 Reset the AP to activate the new configuration.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/reset.asp"
```

11.2 Firmware Updates

CAUTION



Be sure to check for update issues in the new firmware Release Notes.

CAUTION



When using a service controller in conjunction with one or more autonomous APs, you must (1) always upgrade the service controller before upgrading the APs, and (2) never load an earlier firmware version on the APs than is installed on the service controller.

To update AP firmware, select **Maintenance > Firmware updates**.

Figure 11-2: Firmware Updates

NOTE

Configuration settings are preserved during firmware upgrades.

11.2.1 Immediate Update

To update the AP firmware now, **Browse** to the firmware file (extension .cim) and then select **Install**.

NOTE

At the end of the firmware-update process, the AP automatically restarts, causing all users to be disconnected. Once the AP resumes operation, all users must reconnect.

11.2.2 Scheduled Update

The AP can automatically retrieve and install firmware from a local or remote web site identified by its URL.

To schedule firmware installation, follow this procedure:

- 1** Enable **Scheduled install**.
- 2** For **Day of week** select a specific day or **Everyday** and set **Time of day**.
- 3** For **URL**, specify an ftp or http address like this:
 - » **ftp://username:password@192.168.132.11/newfirmware.cim**
 - » **http://192.168.132.11/newfirmware.cim**
- 4** **Validate** the URL.
- 5** To commit the schedule, select **Save**.
- 6** Or, to commit the schedule and also update the firmware immediately, select **Save and Install Now**.

NOTE

At the end of the firmware-update process, the AP automatically restarts, causing all users to be disconnected. Once the AP resumes operation, all users must reconnect.

NOTE

Before a scheduled firmware update is performed, only the first few bytes of the firmware file are downloaded to determine if the firmware is newer than the current. If it is not, the download stops and the firmware is not updated at this time.

11.2.3 Updating Firmware with cURL

NOTE



This is an advanced topic. It is recommended that you upgrade firmware as described in the immediately-previous sections [Immediate Update](#) or [Scheduled Update](#).

You can perform firmware-update-related tasks using the free tool cURL (<http://curl.haxx.se/>), version 7.1.0 or higher.

The following cURL commands shows you how to manage the firmware file. The following setup is assumed:

- IP address of the port 1 is 24.28.15.22.
- Management access to port 1 is enabled.
- Firmware file is **AP.cim**.

Upload the firmware as follows:

- 1 Prepare the AP to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

- 2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
-d pw=admin
```

- 3 Prepare the AP to receive the firmware update.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/firmware_init.asp"
```

- 4 Upload the firmware. Once the upload is complete the AP will automatically restart.

```
curl -s -k --cookie cookie.txt -F firmware=@AP.cim -F backup=Install
"https://24.28.15.22/
    goform/ScriptUploadFirmware"
```

11.3 Licenses

Applicable only to the Wi² AP.

On some APs, certain features are activated by installation of optional licenses. Such features are only enabled when a valid license is installed.

If you purchased an optional-feature license at original AP purchase time, the license is factory-installed. Feature licenses purchased later must be installed manually.

Select **Maintenance > Licenses**. Example from Wi² AP is shown.

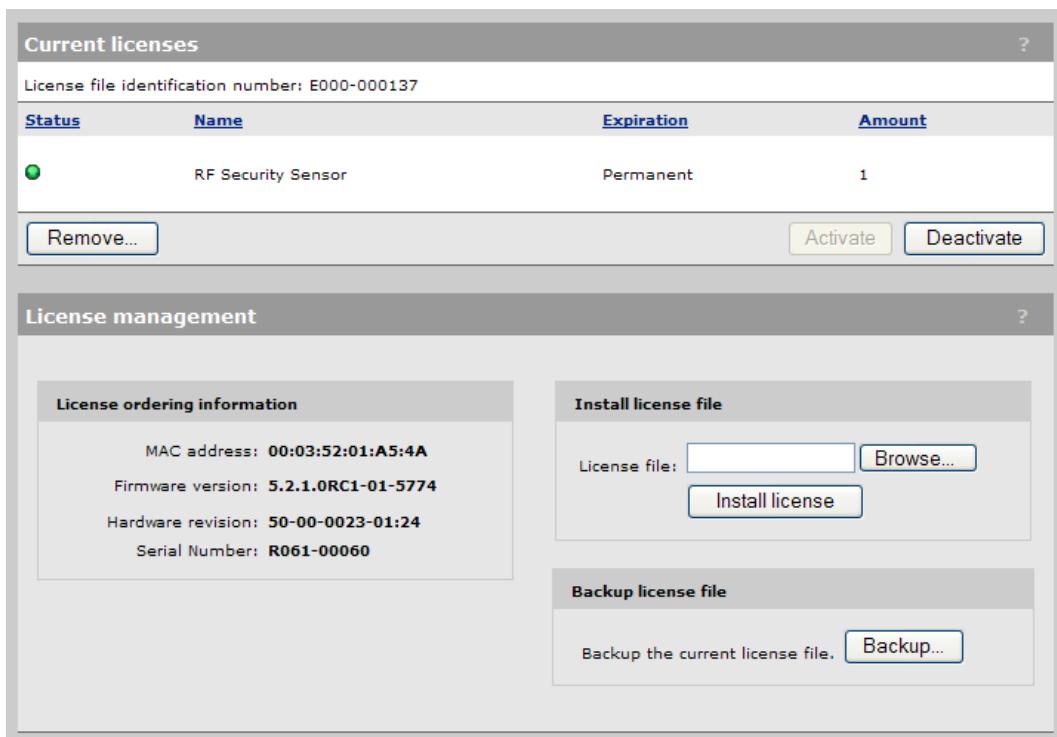


Figure 11-3: Current Licenses

Work with licenses as follows:

- To temporarily deactivate all licenses, select **Deactivate**. Later, select **Activate** to reactivate them.
- To remove all licenses, select **Remove** and then at the prompt, select **OK**.

NOTE

Before removing licenses, be sure to first backup the license file to your hard drive, using the **Backup** button.

- To order a new feature license, provide all information in the **License ordering information** box to your vendor.
- To install a license file, **Browse** to the file and then select **Install License**.
- To backup all licenses into a single file, select **Backup**.

11.3.1 Factory Reset Considerations

After a factory reset, factory-installed licenses are automatically re-activated but user-installed licenses remain in a deactivated state until manually activated. This is done to ensure a true factory-default reset. As shown here, automatically-reactivated factory-installed licenses are shown in the **Current licenses** table. All licenses are shown in the new **Installed licenses** table.

! Due to a configuration reset, your previous licenses have been deactivated and factory licenses have been activated.

Current licenses			
?			
License file identification number: P000-000437			
<u>Status</u>	<u>Name</u>	<u>Expiration</u>	<u>Amount</u>
●	L2 and L3 mobility	Permanent	1
Remove...		Activate	Deactivate

Installed licenses			
?			
License file identification number: E000-000653			
<u>Status</u>	<u>Name</u>	<u>Expiration</u>	<u>Amount</u>
○	RF Security Sensor	Permanent	3
○	L2 and L3 mobility	Permanent	1
Restore			

Figure 11-4: Factory Reset

To activate all user-installed licenses, select the **Restore** button. Table **Controlled licenses** is updated to include the user-installed licenses and the **Installed licenses** table disappears.

The screenshot displays two main sections: 'Current licenses' and 'License management'.

Current licenses:

Status	Name	Expiration	Amount
Green circle	L2 and L3 mobility	Permanent	1

Buttons: Remove..., Activate, Deactivate.

License management:

- License ordering information:**

MAC address: **00:03:52:08:05:04**
Firmware version: **5.2.2.30-01-6352**
Hardware revision: **55-01-0022-00:25**
Serial Number: **W044-00056**
- Install license file:**

License file: Browse...
Install license
- Backup license file:**

Backup the current license file.

Figure 11-5: Installed Licenses



A

Appendix A - Troubleshooting

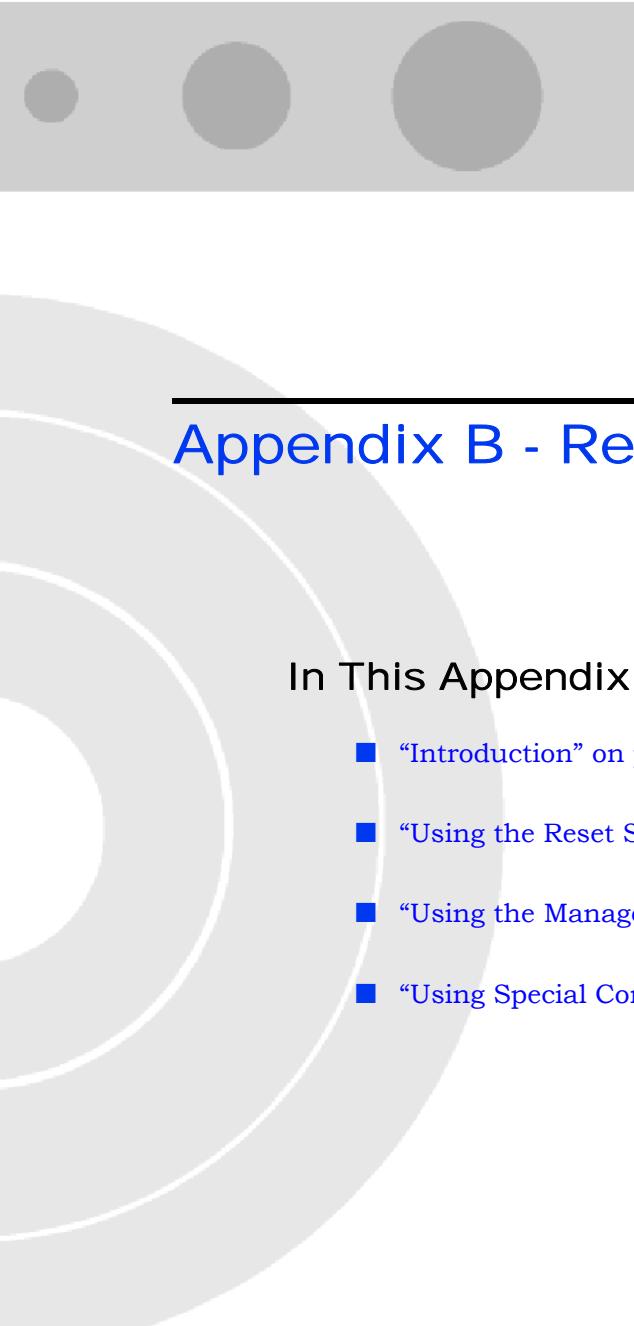
In This Chapter:

This appendix provides a lists of things to check in case of problems before contacting local Technical Support.

Check the following before you contact local Technical Support.

- 1** If wireless clients cannot access the network, check the following:
 - » Be sure the AP and the wireless clients are configured with the same Service Set ID (SSID).
 - » If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
 - » If authentication is being performed through a RADIUS server, ensure that the clients are properly configured on the RADIUS server.
 - » If authentication is being performed through IEEE 802.1X, be sure the wireless users have installed and properly configured 802.1X client software.
 - » If MAC address filtering is enabled, be sure the client's address is included in the local filtering database or on the RADIUS server database.
 - » If the wireless clients are roaming between access points, make sure that all the access points and wireless devices in the Extended Service Set (ESS) are configured to the same SSID, and authentication method.
- 2** If the AP cannot be configured using the Telnet, a web browser, or SNMP software:
 - » Be sure that the AP has been configured with a valid IP address, subnet mask and default gateway.
 - » If VLANs are enabled on the AP, the management station should be configured to send tagged frames with a VLAN ID that matches the AP's management VLAN (default VLAN 1). However, to manage the AP from a wireless client, the AP Management Filter should be disabled.
 - » Check that you have a valid network connection to the AP and that the Ethernet port or the wireless interface that you are using has not been disabled.
 - » If you are connecting to the AP through the wired Ethernet interface, check the network cabling between the management station and the access point. If you are connecting to AP from a wireless client, ensure that you have a valid connection to the AP.

- 3 If you cannot access the on-board configuration program via a serial port connection:
 - » Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.
- 4 If you forgot or lost the password:
 - » Set the AP to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name *admin* and a null password to access the management interface.
- 5 If all other recovery measure fail, and the AP is still not functioning properly, take one of the following steps:
 - » Reset the AP's hardware using the console interface, web interface, or through a power reset.
 - » Reset the AP to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name *admin* and a null password to access the management interface.



B

Appendix B - Resetting to Factory Defaults

In This Appendix:

- “Introduction” on page 216
- “Using the Reset Switch” on page 216
- “Using the Management Tool” on page 216
- “Using Special Commands” on page 218

B.1 Introduction

To force an AP into its factory default state, follow the procedures in this section.

CAUTION



Resetting an AP to factory defaults deletes all configuration settings, resets the administrator username and password to admin, enables the DHCP client on the LAN port(s), sets the IP address of the port(s) to 192.168.1.1.

NOTE



Some of the techniques described in this appendix cause the AP to be forced back into its default controlled mode. If desired, after performing the factory reset, switch the AP back into autonomous mode by following all the directions in “[To perform these initial login tasks](#)” on page 54.

NOTE



Licenses are retained after a factory reset. See “[Factory Reset Considerations](#)” on page 208.

B.1.1 Using the Reset Switch

Not applicable to the ruggedized Wi² AP.

NOTE



This technique forces the AP into its factory default state including switching the AP back into autonomous mode.

Using a tool such as a paper clip, press and hold the reset switch for a few seconds until the front status lights flash three times.

B.1.2 Using the Management Tool

Launch the management tool (default <https://192.168.1.1>).

To reset the AP to factory defaults, **keeping it in autonomous mode**, follow this procedure:

- 1 Select **Maintenance > Config file management**.
- 2 Under **Reset configuration**, click **Reset**.

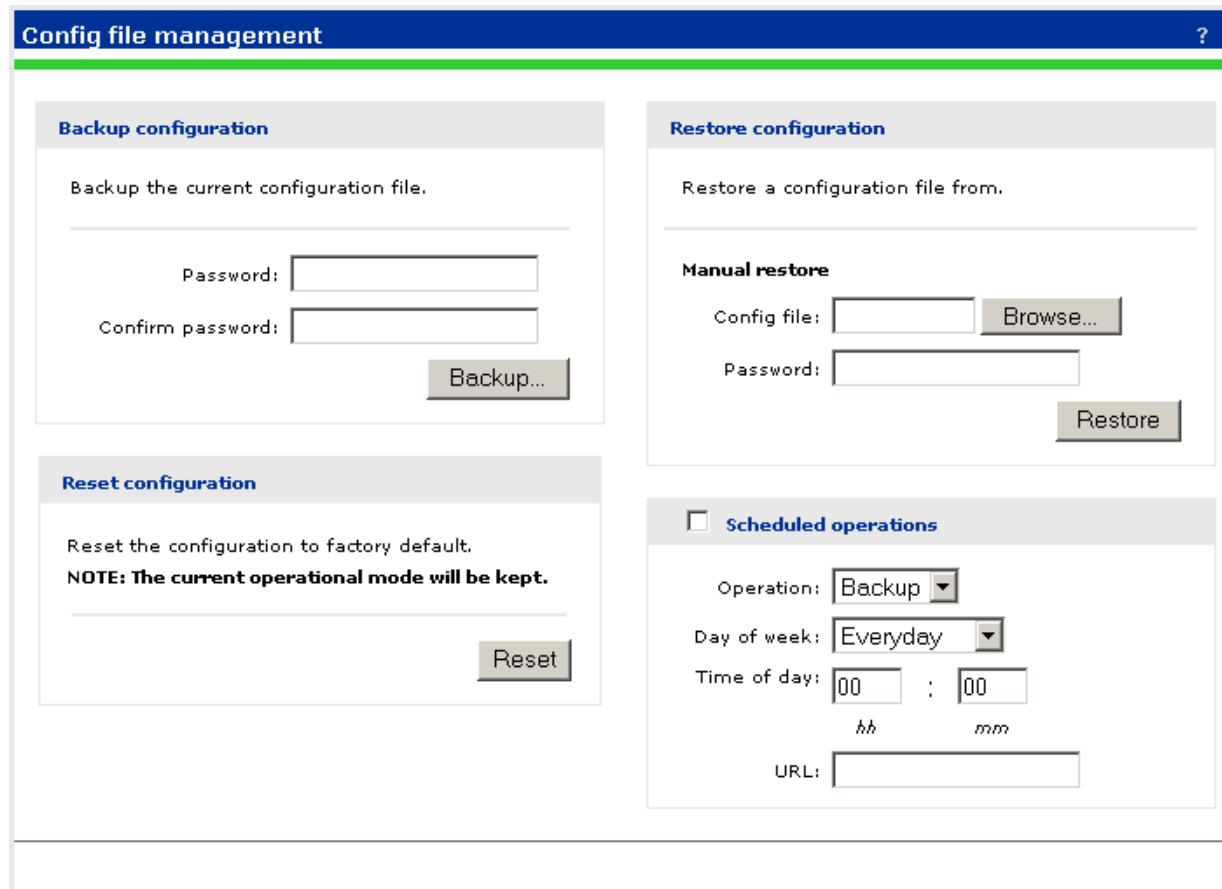


Figure B-1: Config File Management

To reset the AP to factory defaults and **FORCE it back into its default controlled mode**, follow this procedure:

- 1 Select **Maintenance > System**.
- 2 Under **Factory reset**, click **Reset to Factory Default**.

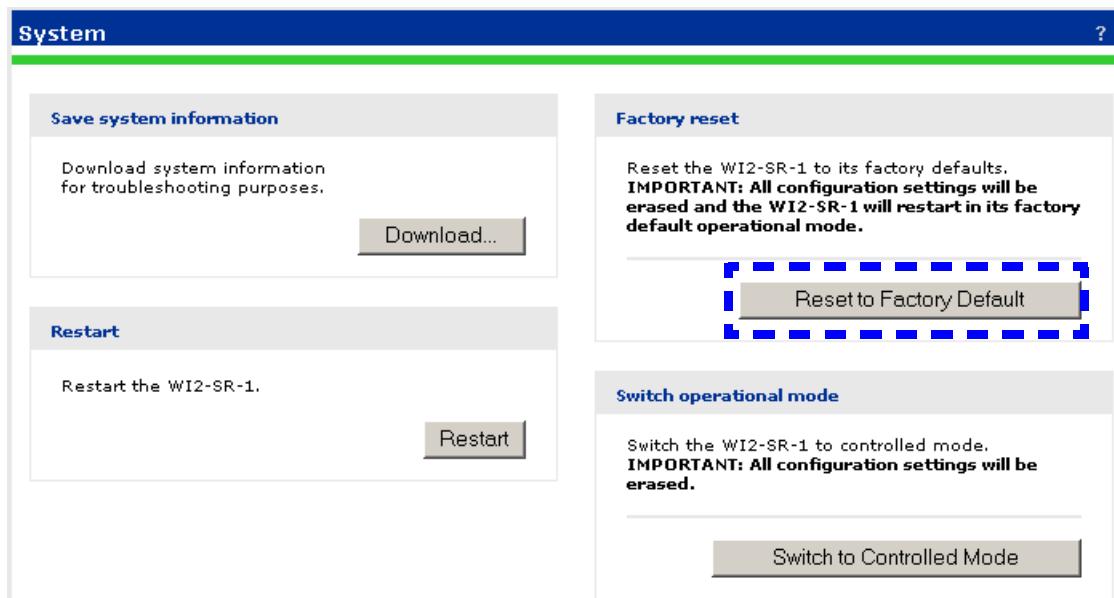


Figure B-2: System

B.1.3 Using Special Commands

NOTE



Follow the directions in this section only for the outdoor ruggedized Wi² AP units **AND ONLY when you do not have access to the unit via its management tool.**

NOTE



This technique forces the AP into its factory default state including switching the AP back into controlled mode.

In addition to the AP, you need the following items:

- » The file **Wi2Remote.bat** available for download from the Alvarion extranet at
<https://extranet.alvarion.com>.
- » A crossover Ethernet cable
- » A standard (not crossover) Ethernet cable

The file **Wi2Remote.bat** runs in a Windows command-line session. It uses this syntax:

```
Remote [factory | restart | cimfile]
```

- Specify `Remote factory` to factory reset the unit.
- Specify `Remote restart` to perform a simple restart (same as powering off and back on).
- The `cimfile` option is used only by technical support personnel for loading special firmware files.

To perform a factory reset, follow this procedure:

- 1 Disconnect any cable from the AP.
- 2 Disconnect power from the PoE injector.
- 3 Configure your computer's LAN port with a static IP address of **192.168.1.2** and a subnet mask of **255.255.255.0**.
- 4 Use a crossover cable to connect your computer's LAN port to the PoE injector **Data In** port.
- 5 Connect a standard Ethernet cable from the PoE injector **Data and PoE Out** port to the AP.
- 6 Open a command line session on the computer.
- 7 Specify `Remote factory` and press **Enter**.
- 8 Power on the PoE injector. The script discovers the AP and causes the factory reset to occur.
- 9 Wait for two minutes for the factory reset to complete and then confirm operation by launching the management tool in a web browser at address **<https://192.168.1.1>**.



Glossary

100BASE-TX	IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.
10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable
802.1p	IEEE 802.1p is a standard that provides traffic class expediting and dynamic multicast filtering
AES	Advanced Encryption Standard: An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.
AKA	Authentication and Key Agreement
AP	Access Point: The device that acts as a communication hub, connecting wireless clients to the network.
Authentication	The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.
Beacon	A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.
Broadcast Key	Broadcast keys are sent to stations using 802.1X dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.
BSS	Basic Service Set: A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.
CA	Certificate Authority
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CDP	Cisco Discovery Protocol

CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
CPE	Customer Premise Equipment: Communications equipment that resides on the customer's premises.
CRL	Certificate Revocation List
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
cURL	cURL automates unattended file transfers or sequences of operations
DHCP	Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.
DiffServ	Differential services: a method for defining IP traffic priority on a per-hop basis.
DNS	Domain Name Server
EAP	Extensible Authentication Protocol: An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the Wi ² , and a RADIUS server.
ESS	Extended Service Set: More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.
FAST	
FTP	File Transfer Protocol: A TCP/IP protocol used for file transfer.
GRE	
GTC	
HTTP	Hypertext Transfer Protocol: A standard used to transmit and receive all data over the World Wide Web.
IAPP	Inter Access Point Protocol: A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant Wi ² s.

IEEE 802.11b	A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.
IEEE 802.11g	A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.
IEEE 802.1X	Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.
LAN	Local Area Network: A group of interconnected computer and support devices.
MAC	Media Access Control: The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and are controlled by the IEEE.
AP	Access Point
MD5	Message-Digest algorithm 5
MPPE	Microsoft Point-to-Point Encryption is a protocol for encrypting data across Point-to-Point Protocol (PPP) and Virtual Private Network links
MSCHAP	Microsoft version of the Challenge-handshake authentication protocol, CHAP
MTU	Maximum Transmission Unit
NAS	Network Attached Storage

NTP	Network Time Protocol: NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.
OFDM	Orthogonal Frequency Division Multiplexing: OFDM / allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.
Open System	A security option for the AP which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest AP.
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol.
PEM	
PHY Type	
PKCS	Public-Key Cryptography Standards
PoE	Power over Ethernet: A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of Wi ² s and network devices, and significantly decreased installation costs.
PPPoE	Point-to-Point Protocol over Ethernet
PSK	WPA Pre-shared Key: PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.
QoS	Quality of Service.
RADIUS	Remote Authentication Dial-In User Service: A logon authentication protocol that uses software running on a central server to control access to the network.
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send

Session Key	Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the Wi ² .
Shared Key	A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMI	
SNMP	Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.
SNR	Signal-to-noise ratio
SNTP	Simple Network Time Protocol: SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.
SOAP	Protocol for exchanging XML-based messages over computer networks, normally using HTTP/HTTPS
SSH	Network protocol that allows data to be exchanged over a secure channel between two computers
SSL	Secure Sockets Layer
SSID	Service Set Identifier: An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).
SU-IDU	Subscriber Indoor Unit
SU-ODU	Subscriber Outdoor Unit
SVP	Spectralink Voice Protocol: an open standard for the prioritization of voice traffic on wireless and wired LANs.
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

TKIP	Temporal Key Integrity Protocol: A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
TLS	Transport Layer Security
TOS	Type of Service: can be used to mark prioritization or special handling for IP packets.
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
VAP	Virtual Access Point: Virtual AP technology multiplies the number of Access Points present within the RF footprint of a single physical access device. With Virtual AP technology, WLAN users within the device's footprint can associate with what appears to be different Wi ² s and their associated network services. All the services are delivered using a single radio channel, enabling Virtual AP technology to optimize the use of limited WLAN radio spectrum.
VLAN	Virtual Local Area Network: A group of devices on one or more LANs that are configured with the same VLAN ID so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Used also to create separation between different user groups.
VPN	Virtual private network
VSC	Virtual network.
WEP	Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.
WPA	WiFi Protected Access: WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.